


Department for Digital, Culture, Media and Sport UK Cyber Security Sectoral Analysis and Deep-Dive Review

A Report by RSM, in collaboration with the Centre for Secure Information
Technologies (CSIT)

June 2018

TABLE OF CONTENTS

EXECUTIVE SUMMARY	1
1. INTRODUCTION & METHODOLOGY.....	2
1.1 INTRODUCTION.....	2
1.2 METHODOLOGY	3
2. ANALYSIS AND REPORTING	7
2.1 DEFINITION OF CYBER SECURITY & ANALYSIS FRAMEWORK.....	7
2.2 PROFILE OF CYBER SECURITY FIRMS.....	8
2.3 EMPLOYMENT	18
2.4 REVENUE	22
2.5 ADDITIONAL CYBER SECURITY RELATED ACTIVITY REVENUES.....	29
2.6 GROSS VALUE ADDED	44
2.7 INVESTMENT LANDSCAPE.....	47
3. REGIONAL ANALYSIS	54
3.1 INTRODUCTION.....	54
3.2 DEFINING ECONOMIC CLUSTERS.....	56
3.3 SELECTING CYBER SECURITY CLUSTERS.....	59
3.4 LIMITATIONS IN CLUSTER ANALYSIS AT REGISTERED LEVEL.....	61
3.5 IMPLICATIONS / RESEARCH APPROACH FOR CLUSTER ANALYSIS	62
4. EXAMPLES OF CLUSTERS	64
4.1 CYBER SECURITY CLUSTERS.....	64
5. UK CLUSTERS: KEY FINDINGS	67
5.1 INTRODUCTION.....	67
5.2 SELECTED CLUSTER SUMMARY.....	70
6. CYBER SECURITY TAXONOMY.....	72
6.1 INTRODUCTION.....	72
6.2 TAXONOMY KEY TERMS	74
6.3 FIRMS BY TAXONOMY	76
7. SURVEY FINDINGS.....	77
7.1 INTRODUCTION.....	77
7.2 RESPONSES.....	77
7.3 KEY FINDINGS	77
8. CONCLUSIONS AND INSIGHT	80
9. APPENDICES	81
9.1 APPENDIX A: SOURCE LIST FOR CYBER SECURITY FIRMS.....	81
9.2 APPENDIX B: TAXONOMY DEFINITIONS AND ORBIS SEARCH TERMS	83



9.3 APPENDIX C: SCORING CRITERIA TO DEFINE FIRMS WITHIN CYBER SECURITY 87

9.4 APPENDIX D: COPY OF CONSULTATION TOPIC GUIDE 88

9.5 APPENDIX E: COPY OF ONLINE SURVEY 91

9.6 APPENDIX F: INVESTMENT FUNDING DEFINITIONS..... 93

9.7 APPENDIX G: RSM RESEARCH METHODOLOGY 94

Disclaimer:

This report has been commissioned by the Department for Digital, Culture, Media and Sport (DCMS) for research purposes.

The information within this report is provided by RSM's Economic Consulting team, in conjunction with the Centre for Secure Information Technologies (CSIT) at Queen's University Belfast and is based upon RSM analysis of the UK Cyber Security industry drawing upon extensive research, official UK company information, interviews with industry, academic and government representatives, and an online survey of cyber security firms promoted by DCMS and RSM in August 2017.

This report offers an estimate of the current state of the UK Cyber Security sector, based upon identification of firms undertaking the production or sale of cyber security products and or services in the domestic market.

As cyber security is an emergent sector which is not well captured in traditional Standard Industrial Classification (SIC) codes, this report and its conclusions and recommendations draw upon a number of economic assumptions, and are therefore advisory in nature.

It is the view of RSM Economic Consulting that this report offers a well-based estimate of the current UK Cyber Security sector. Given the experimental nature of this exercise, we welcome any further feedback or comments on these findings.

Contact Us:

Should you wish to discuss the findings or methodology used for this report in further detail, we would love to hear from you. In the event of any queries, please contact:

Lead Consultant: Sam Donaldson (sam.donaldson@rsmuk.com)

Supporting Consultant: Christian Stow (christian.stow@rsmuk.com)

Associate Director: Jonathan Hobson (jonathan.hobson@rsmuk.com)

The UK group of companies and LLPs trading as RSM is a member of the RSM network. RSM is the trading name used by the members of the RSM network. Each member of the RSM network is an independent accounting and consulting firm each of which practises in its own right. The RSM network is not itself a separate legal entity of any description in any jurisdiction. The RSM network is administered by RSM International Limited, a company registered in England and Wales (company number 4040598) whose registered office is at 50 Cannon Street, London EC4N 6JJ. The brand and trademark RSM and other intellectual property rights used by members of the network are owned by RSM International Association, an association governed by article 60 et seq of the Civil Code of Switzerland whose seat is in Zug.

RSM Corporate Finance LLP, RSM Restructuring Advisory LLP, RSM Risk Assurance Services LLP, RSM Tax and Advisory Services LLP, RSM UK Audit LLP, RSM UK Consulting LLP, RSM Employer Services Limited, RSM Northern Ireland (UK) Limited and RSM UK Tax and Accounting Limited are not authorised under the Financial Services and Markets Act 2000 but we are able in certain circumstances to offer a limited range of investment services because we are members of the Institute of Chartered Accountants in England and Wales. We can provide these investment services if they are an incidental part of the professional services we have been engaged to provide. RSM Legal LLP is authorised and regulated by the Solicitors Regulation Authority, reference number 626317, to undertake reserved and non-reserved legal activities. It is not authorised under the Financial Services and Markets Act 2000 but is able in certain circumstances to offer a limited range of investment services because it is authorised and regulated by the Solicitors Regulation Authority and may provide investment services if they are an incidental part of the professional services that it has been engaged to provide. Baker Tilly Creditor Services LLP is authorised and regulated by the Financial Conduct Authority for credit-related regulated activities. RSM & Co (UK) Limited is authorised and regulated by the Financial Conduct Authority to conduct a range of investment business activities. Before accepting an engagement, contact with the existing accountant will be made to request information on any matters of which, in the existing accountant's opinion, the firm needs to be aware before deciding whether to accept the engagement.

EXECUTIVE SUMMARY



RSM analysis estimates there are currently **846 firms** actively providing cyber security products or services in the UK.



RSM estimate that the cyber security sector's **total revenue in FY2015/16 was £5.7bn.**



RSM estimate that the cyber security sector's **total GVA contribution was £2.3bn in FY2015/16.**



RSM estimate there are c. 31,300– 40,000 staff (FTE) employed in the UK cyber security sector. For transparency, this includes staff within firms providing cyber security products and services, but does not include CISOs, or support staff.



On average, RSM estimate that the sector's revenue per employee in FY2015/16 was **£181,000** and GVA per employee was **£75,000.**



The majority of firms are active in providing **Network Security, Information Risk Assessment & Management** and **Cyber Professional Services.**



89% of the firms are SMEs and collectively drive £1.5bn (26%) of the sector's revenues. The larger firms (11%) earned £4.2bn (74%) in cyber security revenues in FY2015/16.



In the past five years (2012-17), the number of firms active in the sector has grown by over 50%, with **over 100 new business registrations in the market within the past two years, representing a surge in new entrants to the market.**

1. INTRODUCTION & METHODOLOGY

1.1 Introduction

In August 2017, RSM Economic Consulting, in conjunction with the Centre for Secure Information Technologies (CSIT) at Queen's University Belfast, were commissioned by the Department for Digital, Culture, Media & Sport (DCMS) to undertake a sectoral analysis of the UK's cyber security sector.

In March 2018, RSM and CSIT were further commissioned by DCMS to augment the existing sectoral analysis by undertaking additional sectoral revenue analysis and regional cluster analysis, the findings of which have been integrated into this report.

The UK Government has made a clear commitment to its vision for a UK that is 'secure and resilient to cyber threats and is prosperous and confident in the digital world' as set out in the National Cyber Security Strategy (NCSS) 2016-2021. To support the implementation of the strategy, £1.9 billion is being invested in defending national systems and infrastructure, support deterrence of cyber threats, and develop a 'whole-society capability' where all companies and individuals take necessary steps to embed cyber security in their business and personal life.

This study is therefore timely, as it is intended to provide government with an estimate of the current size and scale of the UK cyber security sector. This exercise seeks to review the UK cyber security sector at a detailed and granular level, to ensure an up-to-date economic profile of the sector. This includes the number of UK cyber security companies, the sector's contribution to the UK economy (through revenue and GVA), the number of personnel employed in the sector, and the products and services offered by these firms. This review also explores the investment and funding available to the sector for growth and development, as well as support for training and development and labour supply.

Ultimately, this review offers a current baseline¹ for the economic contribution of the UK cyber security sector. It offers an opportunity for the tracking of progress within the sector, and for further evidence to be gathered to identify barriers to growth.

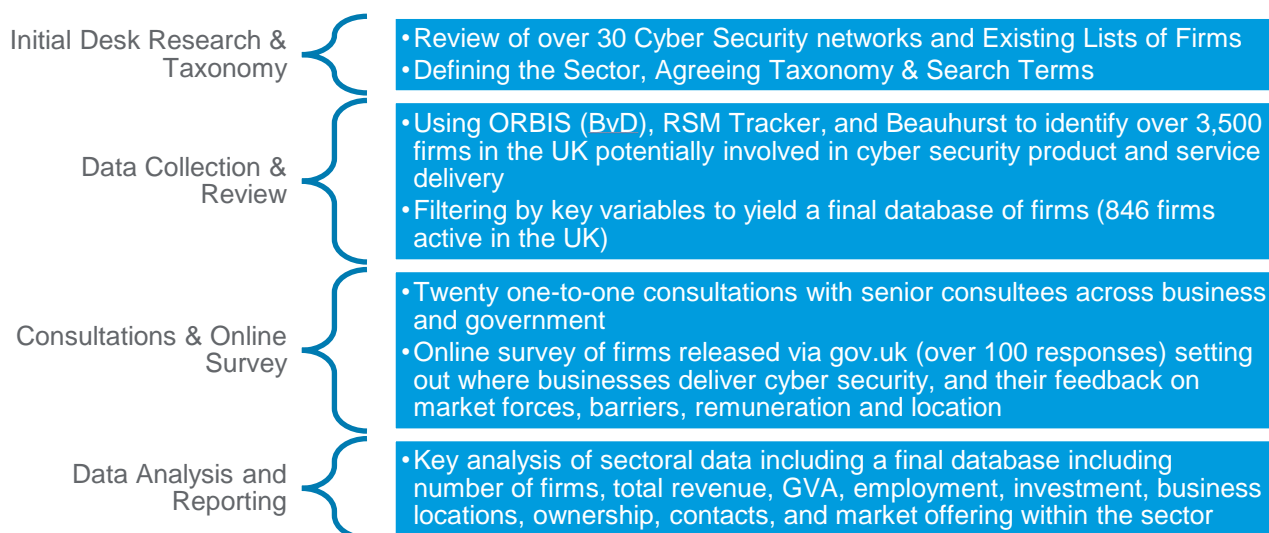
In recognition that the UK cyber security sector does not have a formal Standard Industrial Classification (SIC) code, the approach utilised within this study reflects a defined sector utilising a taxonomy developed by DCMS, in collaboration with the National Cyber Security Centre (NCSC), the Department for International Trade (DIT) and RSM. On this basis, this sector study draws upon experimental statistics, and comments are welcome on the findings of this approach and the underpinning methodology.

¹ Data is based upon reported 2015/16 financial accounts of UK registered firms.

1.2 Methodology

The sectoral analysis involved an extensive programme of data collation, desk based review, and consultation. The data sources used, and research conducted to inform the analysis are set out below, and in further detail in Appendix A.

1.2.1 Summary of the Research Methodology:



This study adopts a ‘bottom-up’ approach to identifying economic activity within the UK Cyber Security sector. It recognises the challenges associated with a ‘top-down approach’ e.g. using SIC codes, which may fail to capture emerging firms within UK cyber security, as well as firms which provide a significant volume of cyber security goods or services but may not typically be considered as a ‘cyber security firm’ e.g. providers of consultancy services. A wide range of data sources were used to inform the study. These include:

Primary Data	Secondary Data	Consultations & Research
<ul style="list-style-type: none"> • Access to over thirty identified networks, clusters and events (listing known cyber security firms, or firms engaged with cyber security sector) • Access to LinkedIn (for real-time identification of firms in 2017, and to inform a profile of firm’s activities and employment by region). 	<ul style="list-style-type: none"> • Orbis (Bureau van Dijk) to collate Companies House data and statements (over 11m UK companies); • RSM Tracker (similar to Orbis, in-house). This provides insight into company turnover, GVA, gross profits, employee remuneration, and location of firms; • Beauhurst, a leading investment analysis platform. 	<ul style="list-style-type: none"> • Approx. 20 one-to-one consultations with leading representatives in the sector from industry, government (national/devolved), and academic partners; • An online survey, promoted by DCMS in August 2017, to collect further data on cyber security activity in the UK

A combination of these sources was used to identify cyber security firms in the UK. These firms were collected through identified networks and clusters, in addition to key search terms (see Appendix B) input into Orbis and Tracker to identify cyber security firms which may report activities within their trade description, but may not be part of an existing network. The database has been tested against the taxonomy of cyber security firms (Appendix B), and each identified firm has been scored to determine sector relevance (see Appendix C for scoring mechanism).

1.2.2 Primary Research

RSM conducted two forms of primary research for this report. This included in-depth telephone interviews with twenty cyber security sector stakeholders to obtain in-depth views of the economic contribution and performance of the cyber security sector, and views on how the sector might be best supported by government. These stakeholders included a broad range of industry subsectors and government departments, across all UK regions.

In addition, an online survey invited individual firms to provide their own data regarding the extent to which cyber security products and services contributed to their firm's revenue and employment, and to provide the regional breakdown of their firm's employment and associated employee remuneration. This was publicised via DCMS, the gov.uk website, social media, and several cyber security networks such as ADS, CyberExchange, and CSIT in August 2017. In total, 107 usable responses² were received.

1.2.3 Defining the sector and identifying businesses

Establishing a long-list of businesses:

The study drew upon a range of sector expertise to identify a list of key search terms for each component within the DCMS Cyber Security taxonomy (see Appendix B). On this basis, the analysis could therefore be further refined in the future subject to any changes in the definition or areas of interest within the Cyber Security taxonomy.

The search terms were subsequently used within Bureau van Dijk's Orbis platform to identify an initial long-list of firms which should be examined as to whether these were to be included in the final dataset i.e. that they were clearly providing cyber security products and services within the UK. The full details of the search terms used are listed in Appendix B, and over two hundred search terms across the taxonomy were explored in the initial identification of potential cyber security firms.

An initial list of over 2,500 firms in the UK was identified using the key search terms in Orbis at the initial research stage. This list of firms was subsequently added to the list of firms identified from source lists provided by DCMS and CSIT (firms known to have been involved in cyber security activity, exhibitions, forums or the Cyber Essentials scheme). Following the removal of 'duplicates', the initial Orbis search and list of known businesses active in the UK provided a long-list of approximately 3,500 firms for subsequent analysis and testing.

Interim list of cyber security businesses:

The initial long-list of cyber security businesses was refined using a scoring mechanism (Appendix C) to exclude firms that were not deemed relevant to the cyber security sector. The scoring system used a range of weighted fields including identified sources, SIC code, trade description, and product and service description to produce a score of between 0 and 10 for each firm. Firms scoring 0 - 1 were removed, those with scores of between 2 - 6 were manually reviewed by sector experts for inclusion or exclusion, and firms with scores of 7 - 10 were automatically included.³

Based on this approach, the number of firms included in the final analysis was refined to 846.

1.2.4 Approach to Analysis and Reporting

This sectoral analysis follows an experimental approach recognising the limitations in identifying cyber security revenues, employment and GVA using a traditional SIC code approach. As a result, RSM has utilised a number of data sources as well as methodological assumptions to inform the analysis, and provide an overview of the sector.

² Other responses were excluded where most answers were not complete or the respondent did not complete the survey.

³ Note that in some cases firms with a score of 0-2 or 7-10 were manually reviewed if deemed appropriate by the research team e.g. where a firm was identified in many sources, but could not be considered for inclusion due to limited taxonomy alignment.

Following the identification of the short-list of firms, it was important to identify the subsequent constraints of the data available, and to provide clear assumptions to address gaps in data. This stage provided three key research challenges:

1. **Where companies are considered micro or small⁴, firms are only required to provide abbreviated accounts to Companies House.** This means that revenue and employment statistics may not be available. Of the 846 firms identified, 576 (68%) of these did not provide such data to Companies House. Therefore, these firms required estimation and or desk review to establish a more robust overview of their activities and extent of operations.

RSM therefore undertook desk review of all 846 firms, using where possible (by order of preference):

- **Provided firms the opportunity to report** their own revenue, employment and products and services (as a wider firm, and from cyber security products and services) through one-to-one consultation and the online survey (see Appendix E);
 - **Company Annual Reports and online information** to validate their known trade description, products and services, and associated employment and revenue;
 - **Company Profiles on LinkedIn⁵:** This explored staff reported employment with firms (in the UK, and filtered where appropriate by suitable category to filter by staff most likely to be involved in Cyber Security divisions within firms that provide cyber security products and services). This was particularly key to estimating employment in micro firms. Where a small UK cyber security consultancy has limited information via Companies House but has six current employees on LinkedIn, for example, this was used to provide a rounded estimate by each firm.
2. It is recognised that it is **not appropriate to allocate all revenue or employment figures to the sector** of the firms identified where they provide multiple services, as this would provide an over-estimation of the extent to which revenue and employment is attributable to the sale of cyber security products and services. This raised the challenge of identifying where firms are either:
 - **'Fully Dedicated'** i.e. all (100%) of their revenues and employment can be attributed to provision of cyber security products and services;
 - **'Mostly Dedicated'** i.e. more than 75%⁶ of their revenues and employment can be attributed to provision of cyber security products and services; or
 - **'Diversified'** i.e. less than 75% of their revenues and employment can be attributed to provision of cyber security products and services.

The extent to which firms were identified as 'dedicated' or 'diversified' was subject to where cyber security employment represented a percentage of the firm's total employment. In other firms, where a firm has twenty employees, that were working to provide cyber security products and services, this firm was considered fully dedicated.

Where a typically larger firm reported that, for example, 500 of their staff (out of a total of 20,000 staff) were working to provide cyber security products and services, this firm would be considered 'diversified'.

⁴ A company will be 'small' where it has any two of the following conditions: a) a turnover of £10.2m or less b) £5.1m or less on the balance sheet c) has fewer than 50 employees.

⁵ Recognising the potential for 'under-reporting' in LinkedIn due to coverage of accounts; set out in Section 3.3.

⁶ The figure of 75% is used as an RSM assumed cut-off for dedicated/diversified as it is assumed that where firms are diversified, they may still be 'operational' without providing cyber security products or services. This is for research and analysis purposes only to understand how many firms **only** provide cyber security products and services, and their respective contribution to the sector and wider economy.

In the online survey undertaken in August 2017, firms were asked the extent to which their firm's revenue and employment was attributable to cyber security products and services. Firms reported that the relationship between percentage of revenue and percentage of employment was comparable i.e. where cyber security revenue was 60% of all revenues, cyber security employment would reflect 60% of all firm employment. This builds the assumption into our analysis that the relationship between a firm's revenue and employment is linear.

3. **Addressing 'gaps' in data identified.** It is recognised that given the nature of the firms, and reporting requirements, that gaps exist in the official financial reporting of firms (particularly due to abbreviated accounts). Therefore, we set out the approach to estimating sector variables where gaps exist.

Variable	Approach to Gaps
<p>Size of Firm: All the 846 firms are known by 'size' i.e. large, medium, small and micro (see Section 3.2).</p>	<p>There were no gaps in this data. This meant that the parameters of each firm were known (see Table 3.1). This allowed RSM to identify average and median values of known data, and to use this where appropriate to inform estimates of revenue and GVA for firms with gaps.</p>
<p>Employment: RSM undertook desk research into all firms separately (including consultation, desk review and LinkedIn) to estimate each firm's employment.</p>	<p>As RSM estimated each firm's employment and built upon existing databases, this provided an overall employment estimate of the sector and each firm.</p>
<p>Revenue: In addition to use of Companies House data, RSM segmented firms by size to understand estimated typical revenue of firms not required to report revenue based on wider sector performance.</p>	<p>Where employment was known in firms, but revenue was a gap, RSM examined firms (by size) with known revenue and employment data. This provided an estimate of average and median revenue by size of firm. This was used to inform revenue gaps where employment was known e.g. where typical revenue for a micro firm was, for example, £35,000 and this firm had 5 employees, then estimated revenue would be £165,000.</p>
<p>Gross Value Added (GVA): $GVA = \text{Operating profit} + \text{Employee Costs} + \text{Depreciation \& Amortisation}$ Where available with Orbis and Tracker, RSM totalled GVA for known firms.</p>	<p>Where GVA was known at the firm level (for c. 270 firms), this provided a known ratio of GVA-to-Revenue within firm by size e.g. 0.4: 1. This informed GVA by firm size where operating profit, employee costs, depreciation and or amortisation were unknown. This was estimated for all gaps, and a total GVA figure is provided in this analysis.</p>

2. ANALYSIS AND REPORTING

2.1 Definition of Cyber Security & Analysis Framework

In the National Cyber Security Strategy 2016-2021, 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.'

This sectoral analysis uses the NCSS definition alongside a developed cyber security taxonomy (see Appendix B).

Within this report, the analysis focuses upon organisations that:

- Have a clear and attributable presence in the UK market, through a UK registered business;
- Report to Companies House on an annual basis;
- Excludes charities, universities, and national networks for analysis purposes;
- Have identifiable UK employment and/or revenue and GVA; and
- Are considered 'active' at the time of writing.

Further, the firms included within this analysis are those which are deemed to provide (to some extent) cyber security products and/or services. These include:

- Information Risk Assessment and Management;
- Identification, Authentication and Access Control;
- Network Security;
- End-User Device Security;
- Monitoring, Detection and Analysis;
- Incident Response and Management;
- SCADA and Information Control Systems;
- Training, Awareness and Education; and
- Cyber Professional Services.

Other important factors to note in our analysis are that;

- Employment, revenue, GVA and investment are assumed only at the UK level (as identified within domestic accounts/or reporting);
- The financial analysis of firms included within the analysis utilises company information from the most recent available year of accounts (in this report, FY 2015/16 is the modal year)
- All data utilized has been collected over an eight-week period (July and August 2017) and is deemed accurate at time of reporting.

2.2 Profile of Cyber Security Firms

2.2.1 Number of Cyber Security Firms in the UK

Our analysis estimates there are currently 846 firms identified to date in the UK providing cyber security products and services. The following subsections provide a breakdown of these companies:

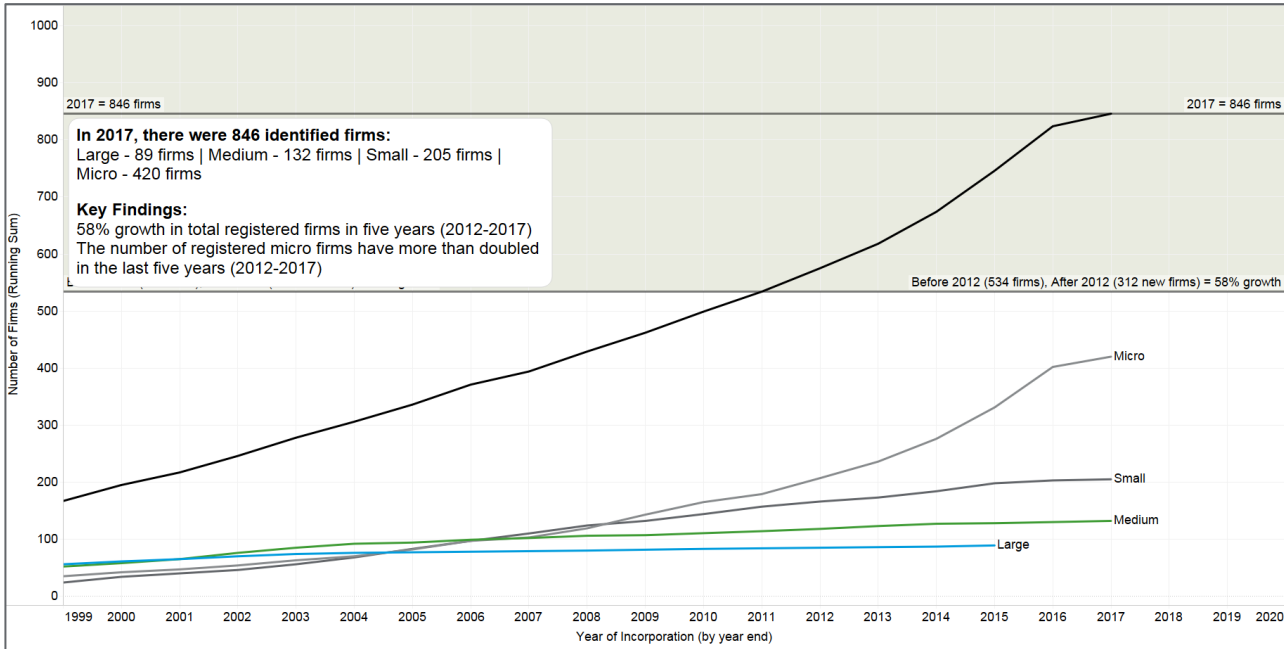
- By incorporation date;
- By geographic region of registered address;
- By company size category;
- By 'dedicated' vs 'diversified'; and
- By products and services; and by SIC codes (at 4-digit level)

2.2.2 By Incorporation Date

Figure 1 sets out all identified firms by registered incorporation date since 1999. Since then, the number of firms involved in cyber security has grown eight-fold, with several companies prior to this date including large multinational firms e.g. BT Group, which have diversified their offer to include provision of cyber security products and services.

However, this analysis provides an interesting overview of how many firms have entered the cyber security market⁷ in recent years. Since 2012, almost three hundred new firms have been incorporated within the sector, representing a 58% increase in the number of firms overall. This has been driven mostly by micro firms (typically fewer than nine employees) with modest growth in small, medium and large firms. This means that the UK sector has experienced considerable activity at the micro level, and represents an area for considerable opportunity and growth, particularly as firms move from start-up into growth positions.

Figure 1 Year of Incorporation (Running Sum), n=846



Source: Bureau van Dijk (Orbis), August 2017

⁷ Please note this examines registration of firms known to the analysis as carried out in August 2017. It does not examine firms which have entered and subsequently 'exited' the market.

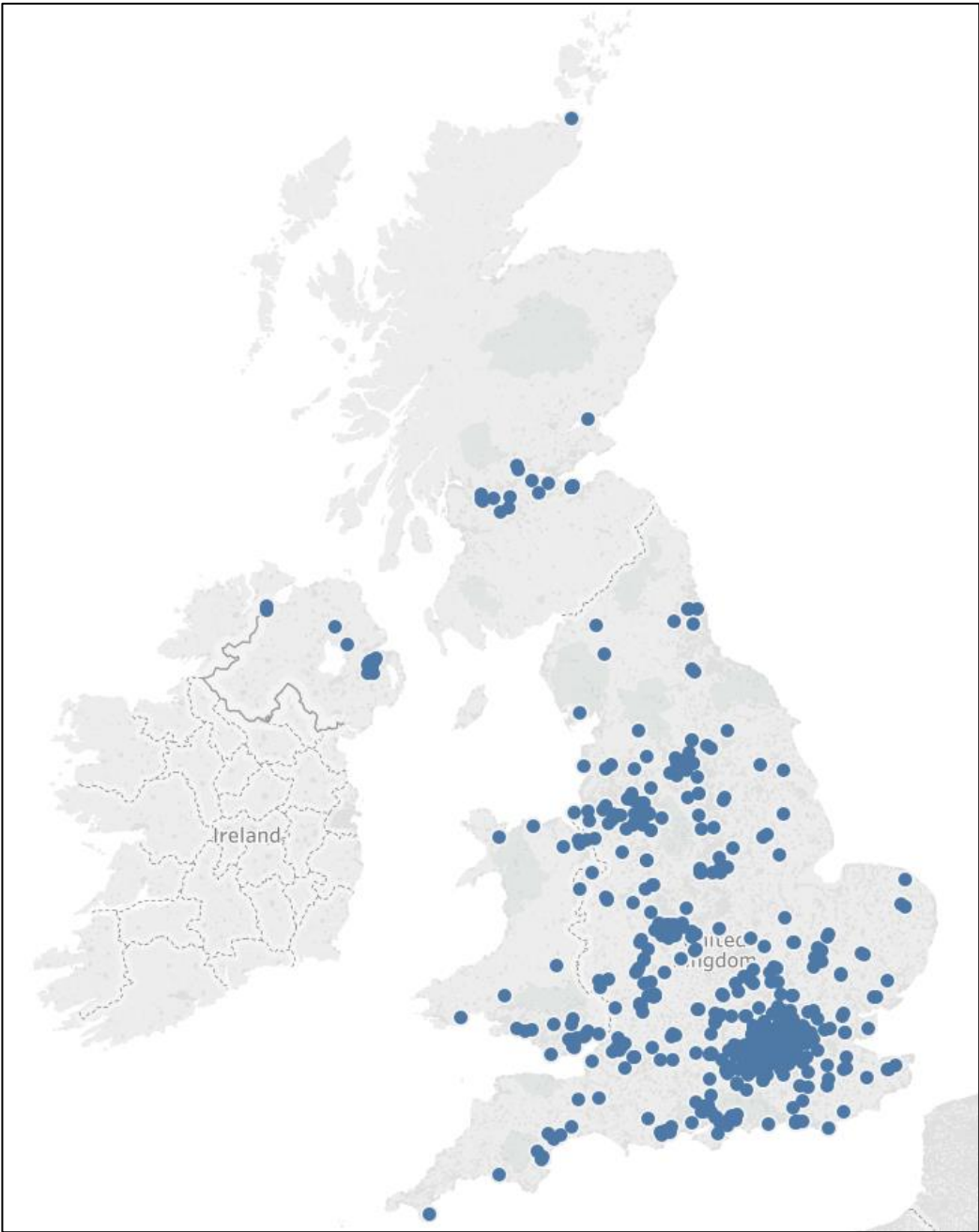
2.2.3 By Geographic Region of registered address

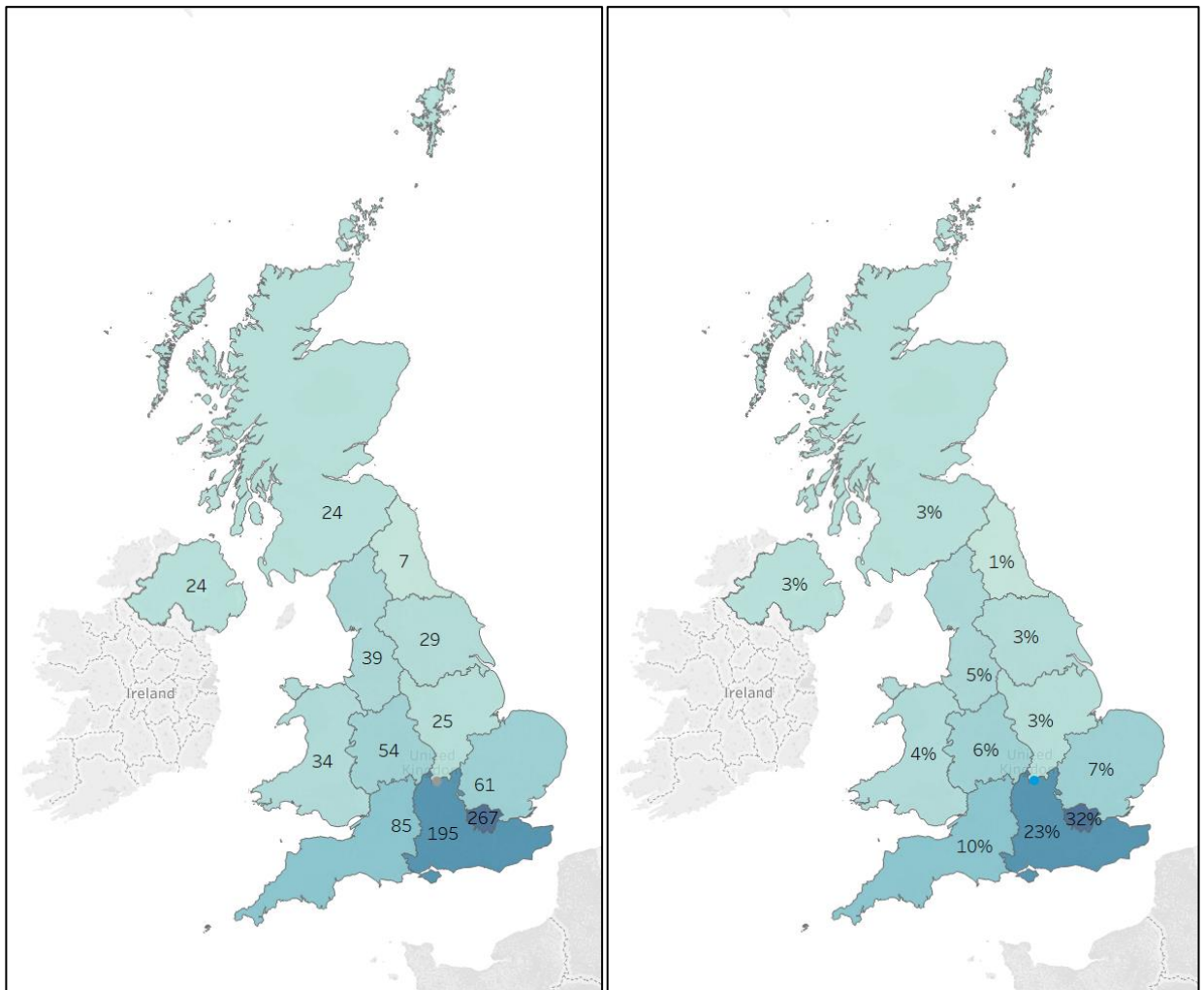
Figure 2 provides a high-level overview of the regional breakdown of companies identified within this study.

This is based upon the Registered Address of active firms in the UK (as of August 2017) and provides a useful insight into where cyber security firms are set-up and registered. However, it captures all firm activity in a single location, which does not fully reflect the dynamics of firms with multiple offices across the UK and/or employees with no fixed location.

As expected, the majority (55%) of firms are registered in London (32%) and the South East of England (23%). This is explored further in Section 2.3 and Section 3 in which we provide an estimate of regional employment, based upon primary and secondary data available to this study.

Figure 2 Registered Location of Cyber Security Companies (Individual, and by Region)





Source: Bureau van Dijk (Orbis), August 2017

2.2.4 By Company Size Category

For the companies identified using Orbis, these are segmented into 'company size categories'.

Table 1: Companies by Size Category

Category	Definition (based on standard EU definitions)	Number of Firms	Percentage
Large Company	Employees ≥ 250 And Turnover $> \text{€}50\text{m}$ or Balance sheet total $> \text{€}43\text{m}$	89	11%
Medium Company	Employees < 250 And Turnover $\leq \text{€}50\text{m}$ or Balance sheet total $\leq \text{€}43\text{m}$	132	16%
Small Company	Employees < 50 And Turnover $\leq \text{€}10\text{m}$ or Balance sheet total $\leq \text{€}10\text{m}$	205	24%
Micro Company	Employees < 10 And Turnover $\leq \text{€}2\text{m}$ or Balance sheet total $\leq \text{€}2\text{m}$	420	49%
	Total	846	100%

This provides a useful indication as to the composition of the 846 firms identified to date as offering cyber security products and/or services:

- Approximately half of firms are 'micro' firms with fewer than 10 employees and either turnover of less than €2m or a balance sheet total of less than €2m.;
- Where companies are 'small' or 'micro', they are usually not required to provide full accounts, which means that revenue and employment statistics may not be available via Companies House. Therefore, these firms require estimation and/or desk review to establish a more robust overview of their activities and extent of operations;
- Where firms are 'large', it is likely these firms offer cyber security products and services as one part of their overall offering. However, they are unlikely to be 'dedicated' to the provision of these products and services, i.e. they may have a few hundred employees providing cyber security advisory services as part of a company with a few thousand employees in total. This is discussed in more detail in Section 2.2.5 below.

2.2.5 By Region and Size

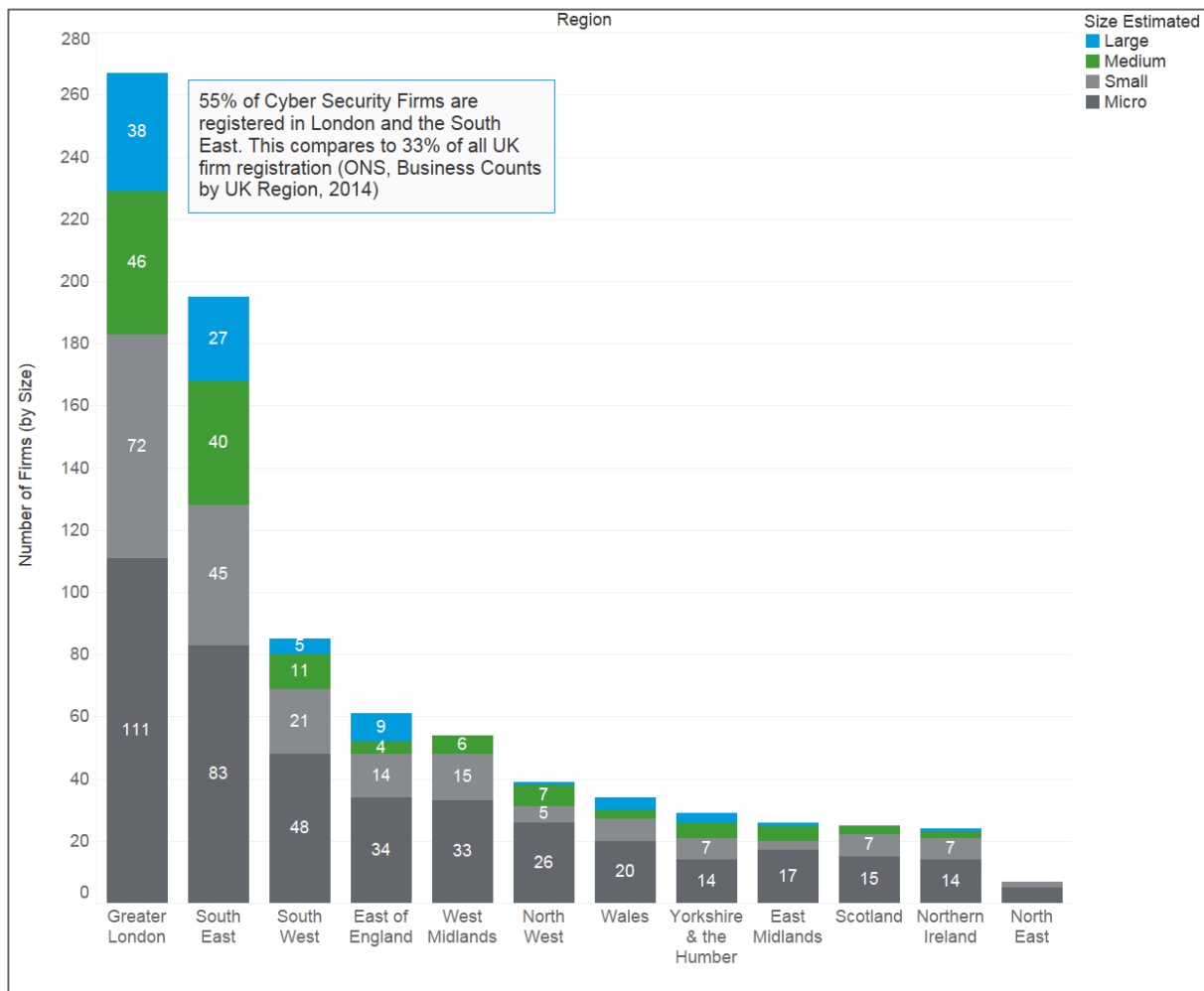
Figure 3 below provides a breakdown of the number of cyber security firms registered by UK region (NUTS1). As noted previously, 55% of the companies are registered in London and the South East⁸. This compares to a figure of 33% of active businesses in the UK being registered in these locations (ONS, 2014).

London has a total of 267 registered (cyber security) firms. Whilst most of these firms are 'small' (69%), London has the lowest proportion of small cyber security firms of any UK region. Further, 38% (n=84) of all 'large or medium' (n=221) firms in the UK are registered in London. This therefore suggests a strong propensity for larger firms to register in London (particularly for international firms with a registered base which is accessible from other international offices).

Please note that, given Orbis extracts data from a firm's 'registered location', this may distort the financial performance data for regions outside of London e.g. where a firm operates in Wales, but is registered in London. This is not unique to this study, and is therefore tested within Section 3 (Regional Analysis) and Section 7 (Survey Findings) to explore the segmentation of business activity across the regions, which is not captured by company reporting data.

⁸ Please note these regions refer to the twelve NUTS 1 (Nomenclature of Territorial Units for Statistics) codes for the UK.

Figure 3 Number of Firms by Region by Size



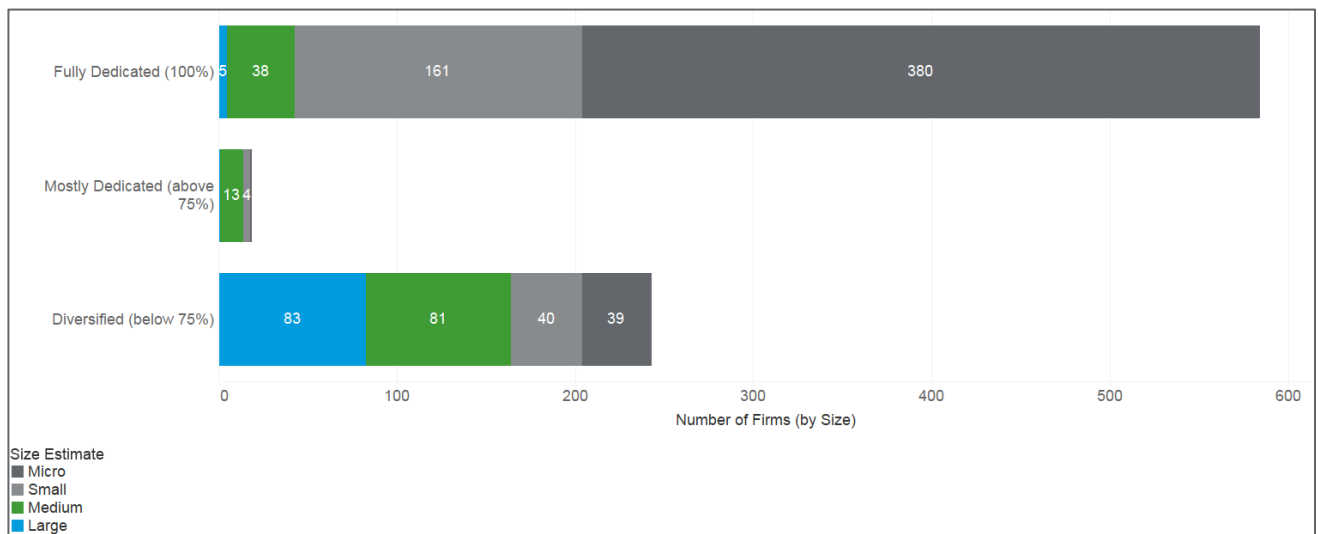
Source: Bureau van Dijk, Orbis, August 2017

2.2.6 By Dedicated and Diversified

This analysis identifies firms which are currently providing some form of cyber security products or services (where aligned to the cyber security taxonomy, see Section 6). This means that 846 firms identified to date are captured regardless of whether all, or less than a percent, of their activities are in cyber security. This is appropriate for providing an aggregated overview of the sector; however, it is important to set out the extent to which companies' employment and revenues depend upon providing cyber security solutions to the market.

Figure 4 provides an overview of the number of firms by size, sorted by the extent to which their activities are dedicated and or diversified in cyber security. This demonstrates that smaller firms are more likely to be 'fully dedicated' and focus on cyber security product and service provision, whereas larger firms are more likely to offer cyber security as a product or service as part of a diversified range e.g. consultancy or IT solutions.

Figure 4 Number of Firms by Size by Dedicated/Diversified



Source: Bureau van Dijk, Orbis, August 2017

Table 2 overleaf sets out how each of these firms have been designated as either ‘fully dedicated’ (whereby all their employment is deemed to originate from cyber security), ‘mostly dedicated (with more than 75% employment)’ or ‘diversified’ (where less than 75% of employment comes from cyber security activity).

The ‘percentage of employment in cyber security’ figure has been estimated for each of the firms identified through the following method:

- Employment figures have been extracted from Orbis where available. Where employment data is not available in company accounts, this has been sourced (by preference) using survey and consultation responses, desk research, and LinkedIn. Where using LinkedIn, a UK estimate has been obtained by filtering UK locations only and cyber security roles have been identified where job descriptions match the key terms associated with the taxonomy.

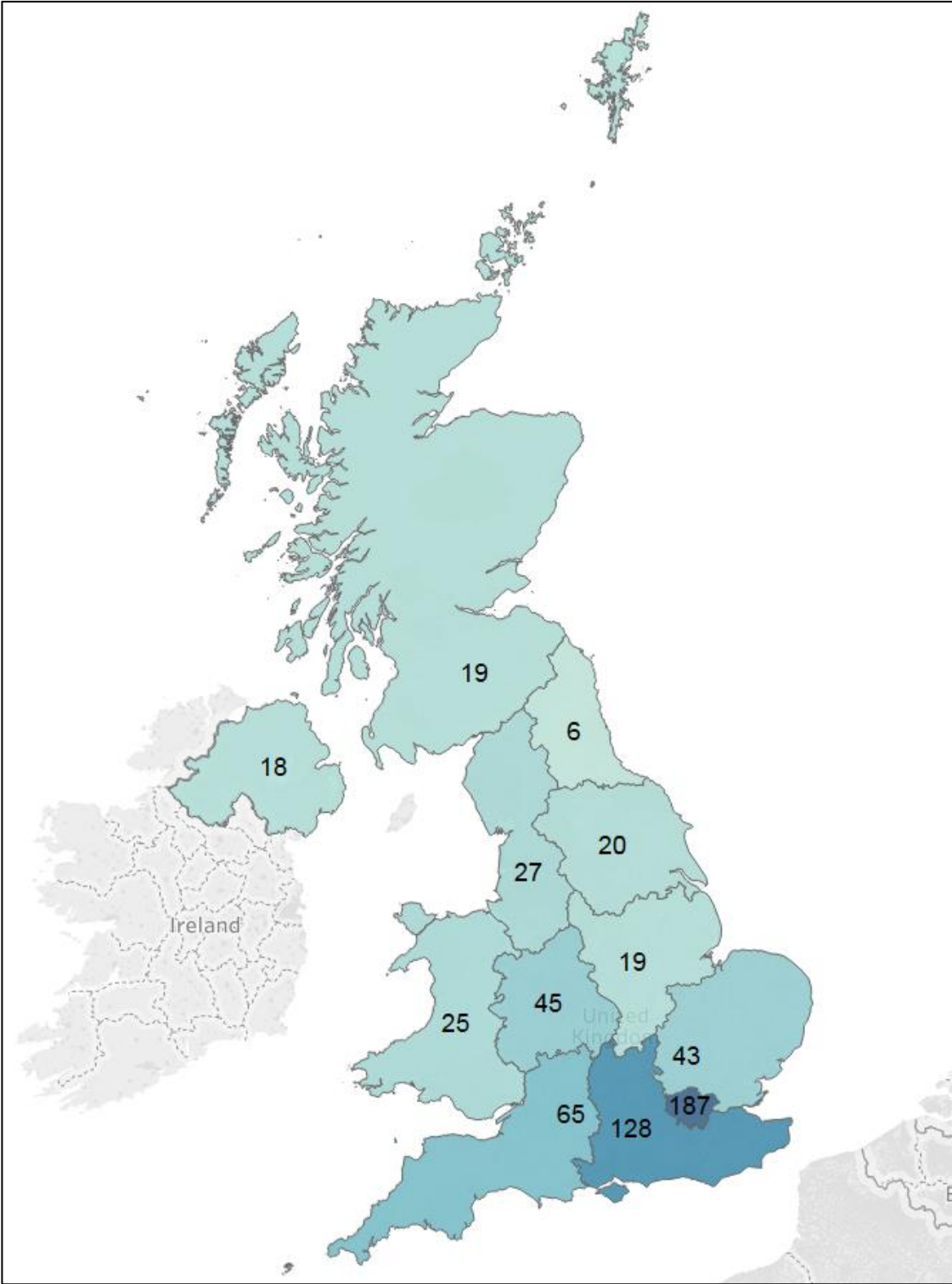
Table 2 Firms by Dedicated and Diversified

Category	Description	No. of Firms	% of Firms
Fully Dedicated (100%)	<p>Companies where RSM estimated (or Orbis confirmed) that all those employed by the firm are supporting the delivery of a cyber security product or service.⁹</p> <p>For example, where a firm reports 100 employees in the UK, and it is clear the firm has a unique purpose in providing 'anti-virus software', it is assumed these employees are in place because of the activities of the firm.</p> <p>For analysis purposes: 'If this company did not provide their cyber security products/services, would they be employing staff to provide other products/services? If the answer is 'no', then the assumption is these firms are fully dedicated.</p>	584	69%
Mostly Dedicated (=>75%)	<p>This relates to companies where RSM estimates that employment data within cyber security activities reflects most the firm's activities (>75%) but not all the activities.</p> <p>Whilst there are a small number of these firms in the overall profile, we consider this an important distinction to identify to explore how these firms change their offering in the future. In addition, it may also be interesting to explore further whether these firms have started off in cyber security and expanded into other areas as part of their offering or made a significant change reflecting market forces.</p>	19	2%
Diversified (<75%)	<p>It is understood that these firms deliver cyber security products or services as a part of their overall business, with the proportion of employment attributed to the cyber products or services accounting for up to 75% of the total workforce. For example, if a consultancy firm employs 3,000 staff in the UK and has an estimated 150 staff in a cyber security advisory/threat monitoring unit.</p>	243	29%
	Total:	846	100%

⁹ This means that where the total number of a company's workforce includes support functions for the business to provide cyber security products or services, this is included in the overall analysis headcount data, as these functions are a required component of the business operations.

Figure 5 sets out a regional overview of registered firms which are considered 'dedicated' cyber security firms, with the majority (53% based in London and the South East). Further analysis (e.g. employment, by dedicated/diversified) is set out further in the remainder of this report.

Figure 5: Number of Firms by 'Dedicated'



Source: Bureau van Dijk, Orbis, August 2017

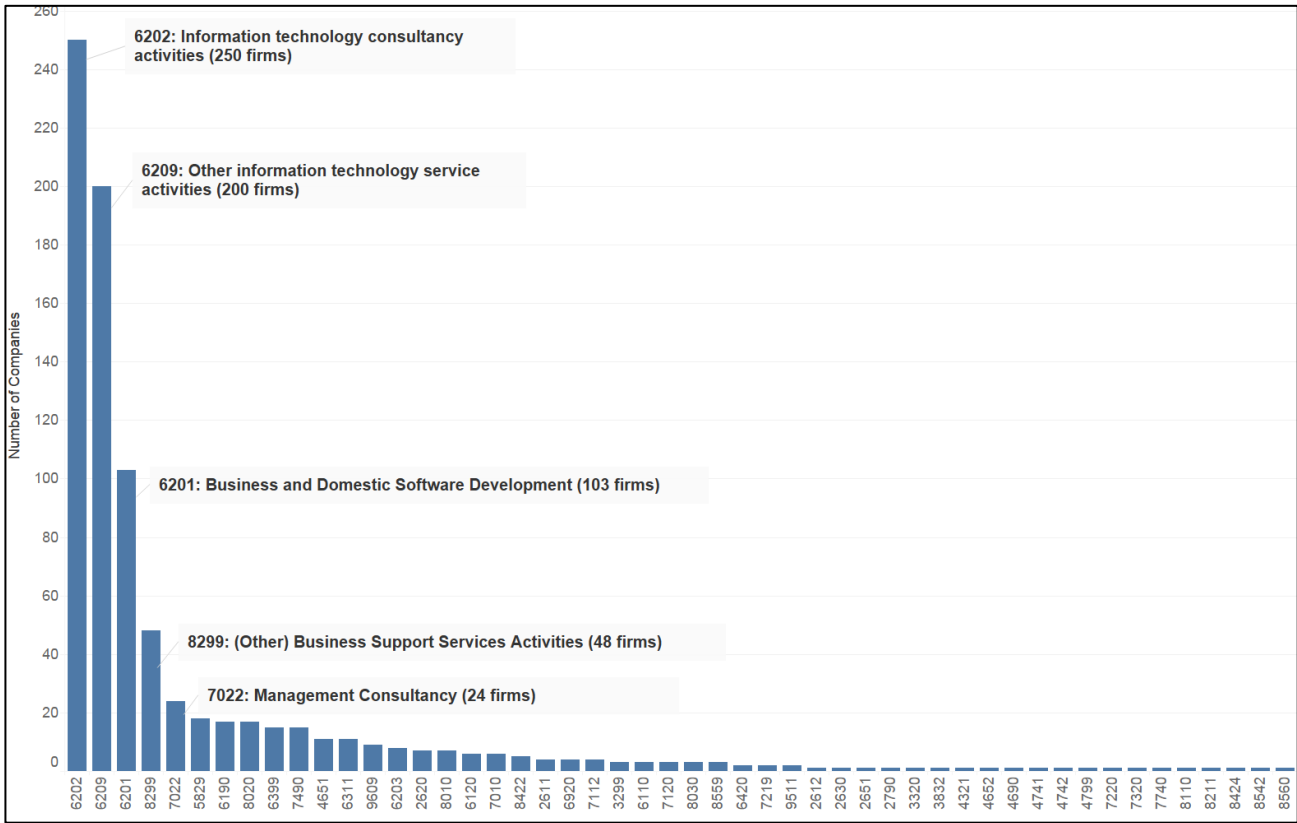
2.2.7 By SIC Codes

Figure 6 sets out the number of firms by 4-digit SIC code. This suggests over two-thirds (68%) of firms are aligned to SIC code 62 (Information Technology), which is expected given cyber security’s role as an underlying sub-sector. However, this analysis does highlight many firms not within SIC 62 which are providing cyber security products and services; most particularly ‘8299’ (Other Business Support), and 7022 (Management Consultancy).

However, whilst these provide a useful initial categorisation of firms (and a layer of validation), these remain vague, and do not fully capture the activities of each firm. Given the nascent nature of the cyber security sector, and that several key firms are not aligned to SIC62, this demonstrates that for a sector such as cyber security, analysis by SIC code is not sufficient to provide an accurate insight to sectoral performance.

Therefore, this highlights why the taxonomy and analysis of full trade description and products and services sold is important for this analysis (highlighted in Figure 7), as this sectoral analysis seeks a more granular understanding of what cyber security products and services are offered by firms active in the UK.

Figure 6 Number of Firms by SIC Code (4 Digit)



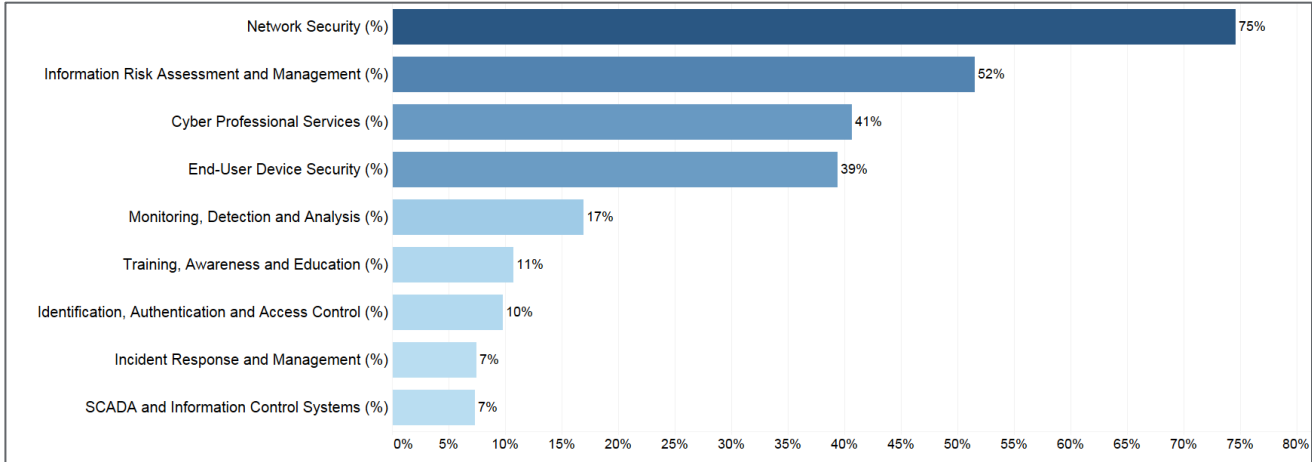
Source: Bureau van Dijk, Orbis, August 2017

2.2.8 By Products and Services

Within this study, RSM has utilised a taxonomy of nine key categories (set out in further detail in Section 6). Where each firm’s ‘Trade Description, or Products and Services’ in Orbis (or where not available in Orbis, via desk review) has matched a ‘key term’ in a component of the taxonomy, this is counted as a single match.

Figure 7 illustrates what percentage of each of the 846 firms matches against the taxonomy ‘key terms’. For example, 74% (n=625) of the firms identified appear to provide products and services aligned to ‘network security’ at a high-level. This exercise is based upon matching of terminology, and therefore dependent upon the language used to refer to firms. It is therefore illustrative of the extent to which cyber security firms identified match against the taxonomy and provides insight into which areas of the taxonomy may have more firms than others e.g. it is estimated that cyber professional services as a market has greater saturation than ‘SCADA and ICS’.

Figure 7 Taxonomy ‘Matches’ in Identified Firms (n = 846)



Source: Bureau van Dijk, Orbis, August 2017

2.3 Employment

2.3.1 Cyber security employment (total)

Our analysis of the 846 firms identified to date as providing cyber security products and services, estimates a total employment figure of 31,339 in cyber security.

Where possible, our analysis utilises company reporting data for employment estimates. Where gaps exist, we have utilised consultation, desk review and LinkedIn to estimate employment.

We recognise that LinkedIn may only provide a representation of employment in the UK, as it is based upon the level to which professionals in the sector engage with the platform and have an account. Further, there is a small risk that employee numbers via LinkedIn may identify counts of employees who may no longer be employed by that firm e.g. where a user has 'two current employers'.

LinkedIn has an estimated 20m users in the UK. There are an estimated 32m people currently employed in the UK¹⁰. This suggests a LinkedIn coverage rate of 63% of the employed population. Given the nature of IT professionals (degree-educated, working in industry settings with need for a work-based communication platform), we estimate as a high level that 80% of cyber security professionals in the UK may be covered by LinkedIn.

Therefore, as an upper estimate to reflect potential 'under-identification' of employment, we apply an uplift of 20% (absolute, 25% relative) to account for cyber security professionals in the UK not being covered by LinkedIn. This provides an increase of 7,835 employees.

Therefore, we estimate that cyber security employment in the UK is in the region of 31,339 – 39,174 employees (FTE)¹¹, the 39,174 figure inclusive of the uplift applied to LinkedIn estimates.

For purposes of subsequent analysis, we use the conservative estimate (identified through RSM analysis) of 31,339.

¹⁰ Office for National Statistics (2018) 'Employment and Employee Types (LFS)' Available at: <https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/employmentandemployeetypes>

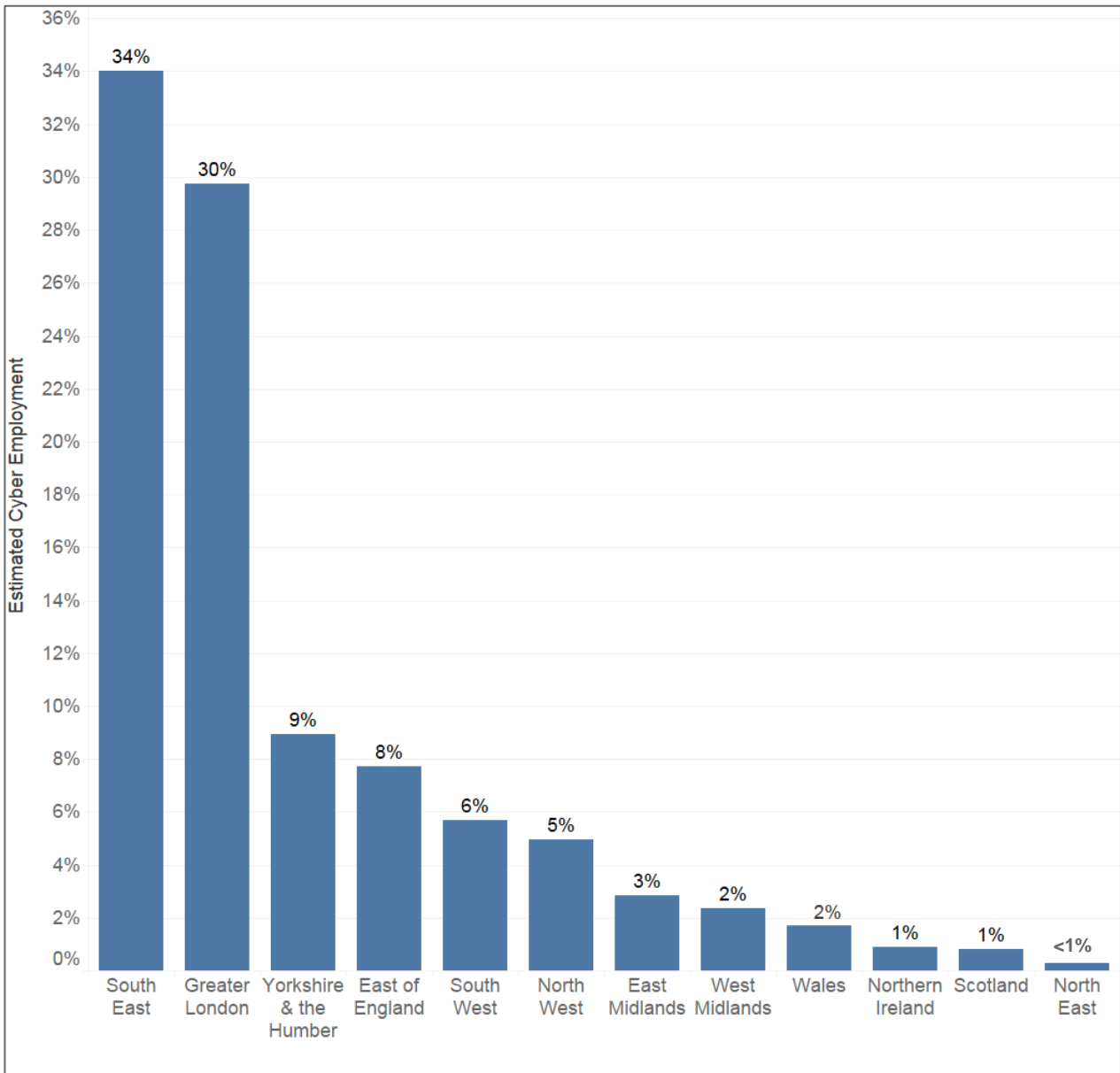
¹¹ 31,500 – 40,000 for rounding purposes.

2.3.2 By Geographic region

As discussed in Section 2.1, we have examined the geographic location of each cyber security firm as per their registered address. However, as this captures all firm activity in a single location, it does not fully reflect the dynamics of firms with multiple offices across the UK and/or employees with no fixed location. This should be taken into consideration alongside the analysis presented in the rest of this section.

Further analysis at a company level could be undertaken in future to understand in detail the regional split of activity and employment for companies with multiple locations across the UK.

Figure 8 Employment by Region



Source: BvD, Orbis, LinkedIn Estimates (RSM), August 2017

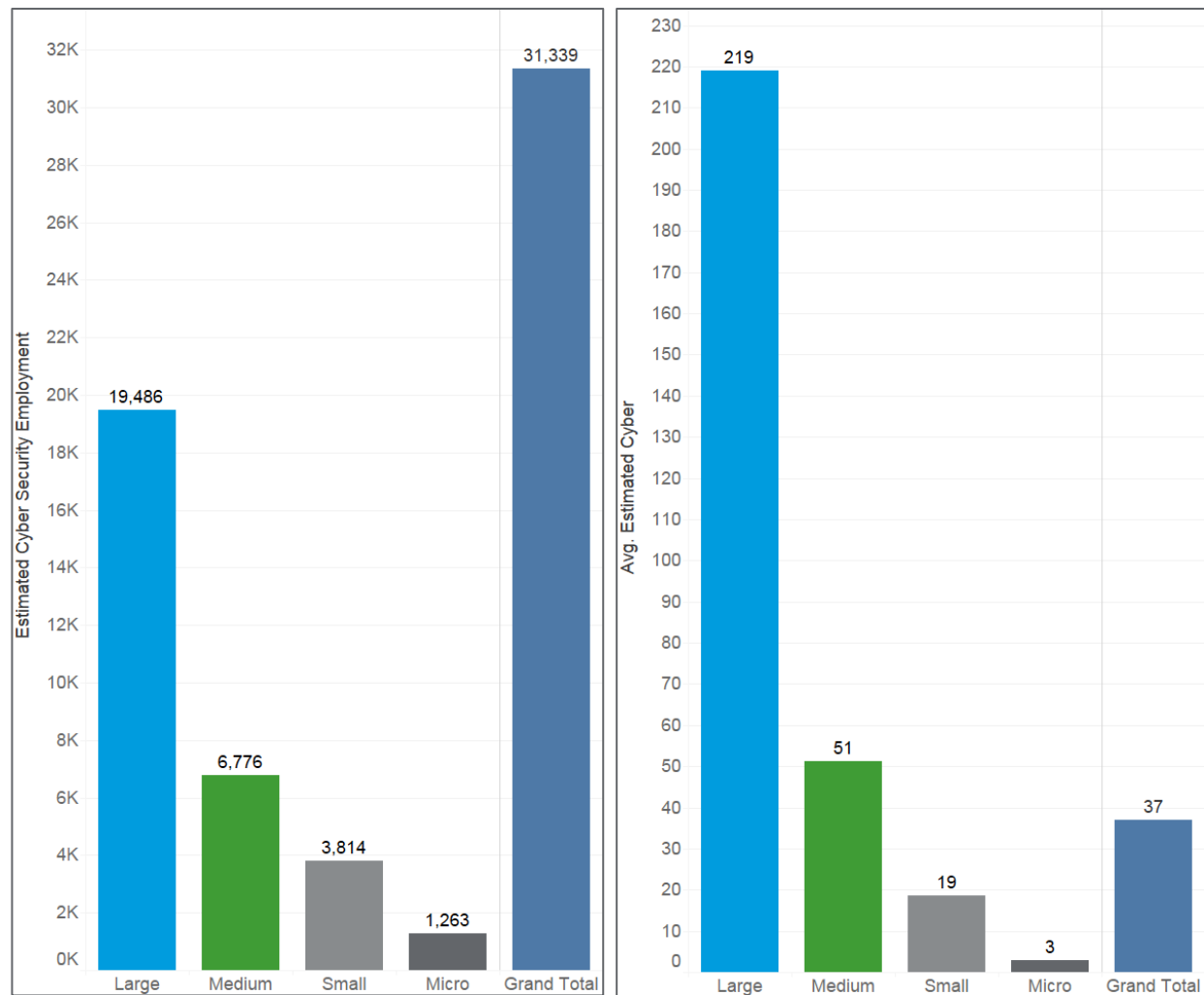
Based on a company’s registered address, we estimate that the South East and London, as expected, account for the greatest share of employment with 34% and 30% respectively. However, it is likely that many regional firms will have a registered address in these regions but will undertake a significant amount of their activity elsewhere in the UK.

2.3.3 By Company size category

Figure 9 sets out employment by company size. Over half (62%) of the employment in cyber security is based in large firms, with the remaining 38% in SMEs.

Overall, employment in the sector is driven by large firms (average of 219 employees related to cyber security products and service provision). This compares with just three employees per micro firm on average, whereby many firms in the UK may represent sole-trading arrangements or a very small employed team.

Figure 9 Employment by Company Size (Total, and Average)



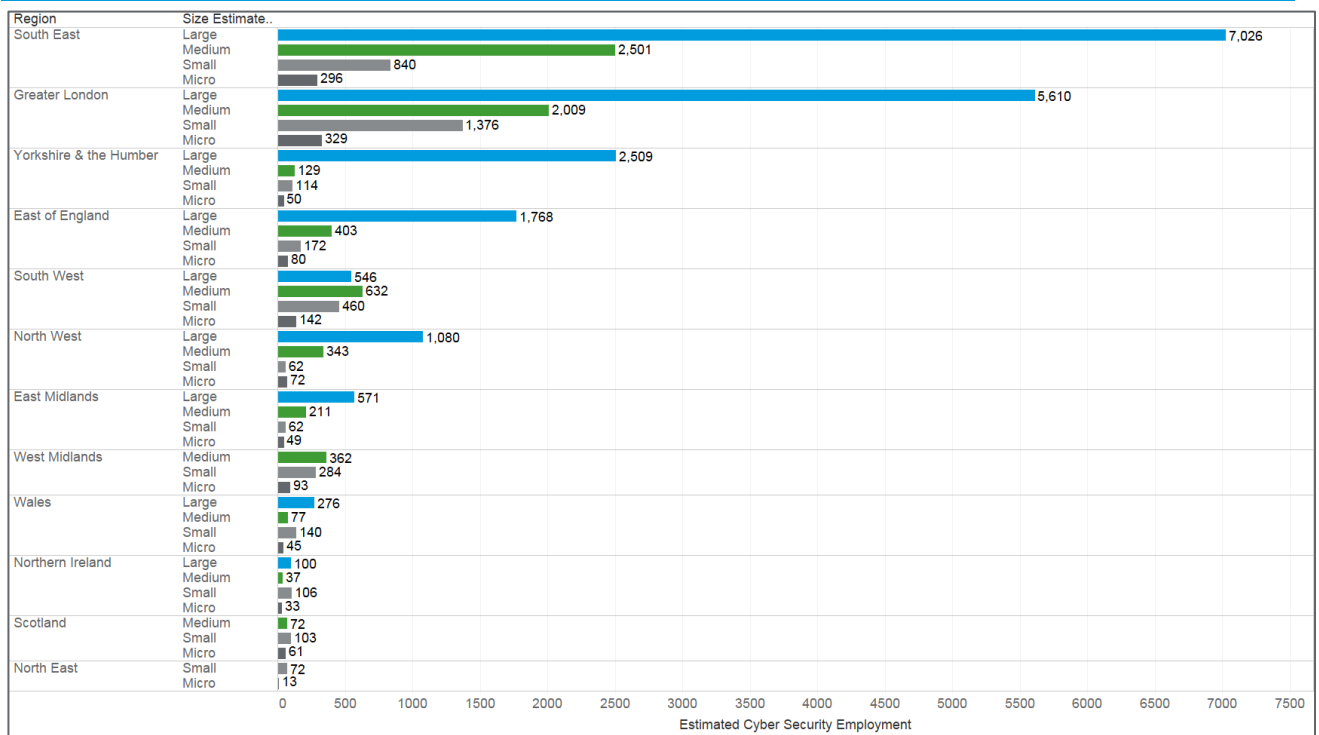
Source: BvD, Orbis, LinkedIn Estimates (RSM), August 2017

2.3.4 Employment by Region and Size

Figure 10 sets out employment by region and size of firm. As expected, many of the large firms in London and the South East are driving overall employment in the sector (c. 7,000 and 5,600 staff respectively). However, this analysis does point to clusters in Yorkshire and the Humber (2,500 in large firms), East of England (1,800) and the North West (c. 1,100).

This estimates employment by **registered location**, and therefore it should be considered alongside Section 3's revised estimates of regional activity i.e. recognising strengths of the sector in Scotland, Wales and Northern Ireland.

Figure 10: Employment by Region and Size



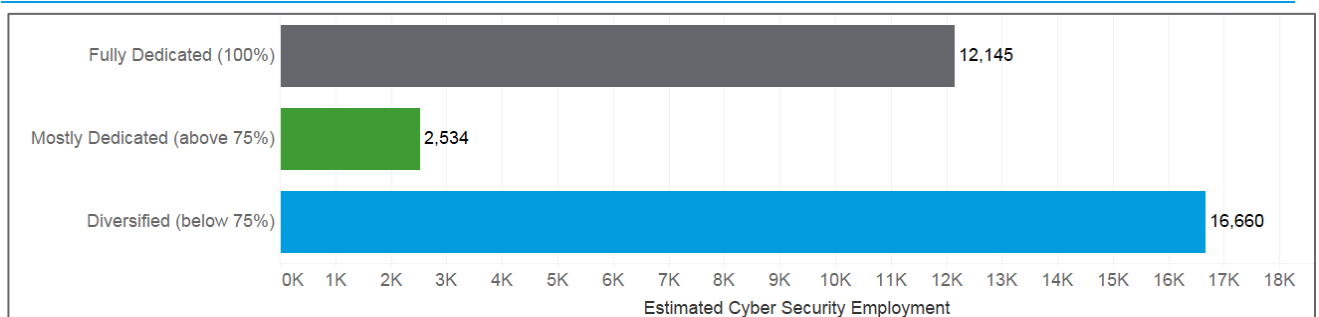
Source: BvD, Orbis, LinkedIn Estimates (RSM), August 2017

2.3.5 By Dedicated and Diversified

Figure 11 sets out employment by 'dedicated' and 'diversified' firms, whereby employment is relatively split by dedicated (47%) and diversified (53%) firms.

However, as there are approximately three times as many dedicated firms as diversified, this suggests that firms identified as dedicated will typically have a smaller cyber security workforce specialising on a particular product or service delivery; whereby larger diversified firms e.g. BAE Systems, BT and Deloitte, have a larger absolute cyber security workforce (in the hundreds) that may still reflect a relatively low proportion of the overall firm structure.

Figure 11 Dedicated and Diversified Employment



Source: BvD, Orbis, LinkedIn Estimates (RSM), August 2017

2.4 Revenue

2.4.1 Cyber security revenue (total)

In the most recent available year (2015/16), cyber security revenue within the sector (846 firms) is estimated at £5,681,730,723 (£5.7bn to the nearest £100m).

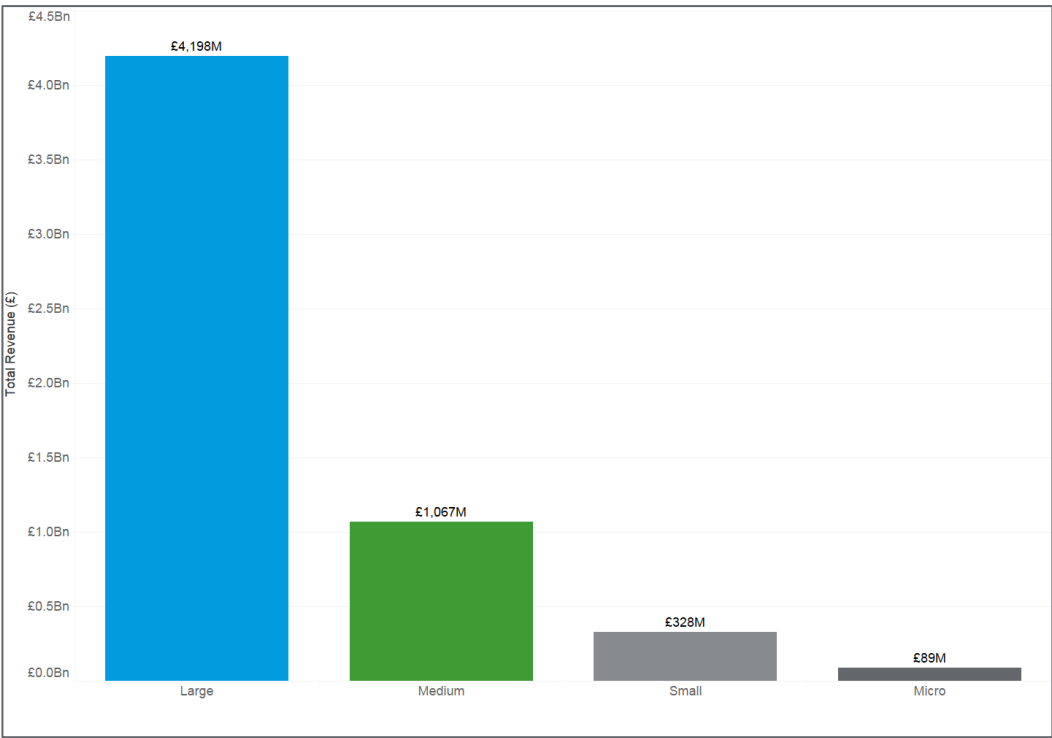
This is based upon the aggregation of revenues of identified firms (weighted by the estimated split of each firm which reflects cyber security revenue). For analysis purposes, each firm’s cyber security employment percentage of overall employment is expected to hold for revenue e.g. where 60% of staff are working in cyber security, it is assumed 60% of revenue comes from cyber security activity.¹²

This revenue estimate relates to the **total estimated cyber security revenue only**, and does not include other revenues reported for diversified firms. This revenue estimate also **excludes** additional revenue earned through other cyber security-related activities (cyber security insurance and internal cyber security functions within organisations) which were quantified in RSM's additional sectoral revenue and regional deep-dive. These estimates are addressed later within this section.

2.4.2 By Company size category

Figure 12 provides a breakdown of total revenue in cyber security by company size. The majority (£4.2bn, c.74%) stems from large firms. For the SMEs, RSM estimates approximately £1.5bn in revenue across 644 ‘medium and small firms’ (est. average revenue of £780,000 per company). This highlights, as per previous analysis of the cyber security sector¹³, that the majority of sector revenue, employment and GVA will be attributable to a small number of ‘large’ firms.

Figure 12 Revenue by Company Size



Source: BvD, Orbis (August 2017)

¹² This has been tested and validated in the RSM online survey of cyber security firms where estimated % of firm employment and firm revenue ‘as cyber’ are comparable.

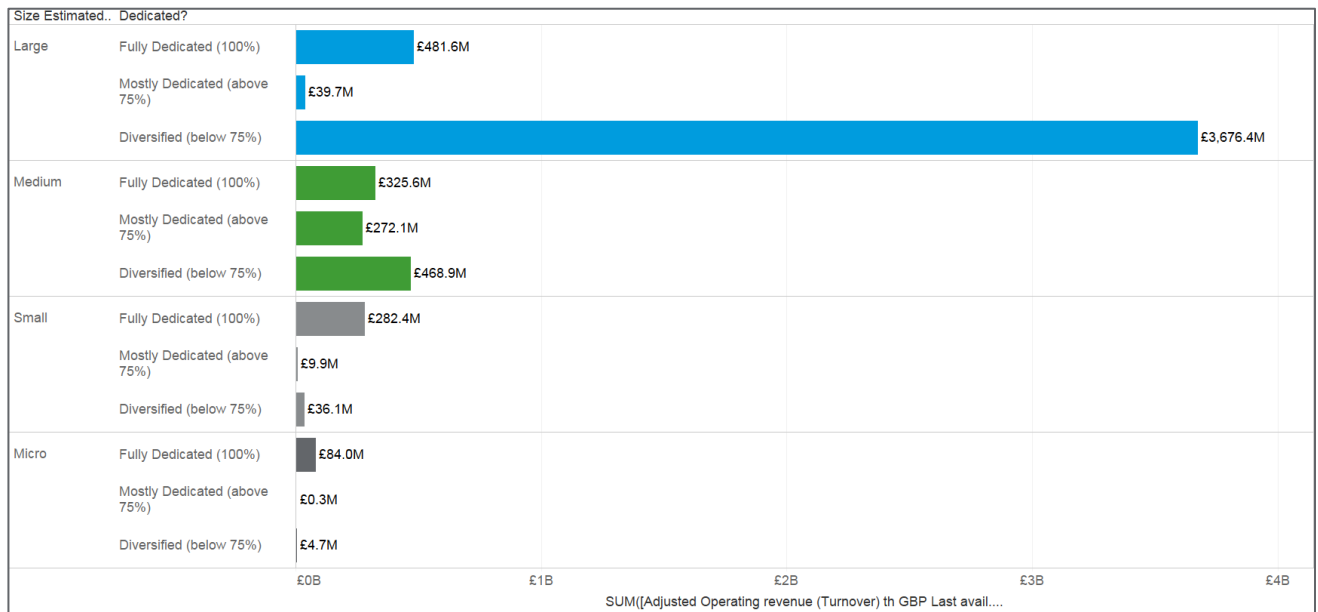
¹³ Pierre Audoin Consultants, ‘Competitive Analysis of the UK Cyber Security Sector’. 2013. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/259500/bis-13-1231-competitive-analysis-of-the-uk-cyber-security-sector.pdf

2.4.3 By “dedicated” vs “diversified”

Figure 13 sets out total revenue within the cyber security sector by firms classified as ‘dedicated’ or ‘diversified’, and by size. The largest proportion of revenue (c. £3.7bn, 65%) comes from large diversified firms e.g. large multinational firms with cyber security representing a significant proportion of their firm, but not their reason for operating e.g. BT, BAE Systems etc.

Where firms are identified as dedicated, large firms have a combined revenue of almost £500m (c. 8% of the sector), followed by medium firms (£326m), small firms (£282m) and micro firms (£84m).

Figure 13 Revenue by Dedicated/Diversified



Source: BvD, Orbis (August 2017)

2.4.4 Previous Cyber Security Sectoral Revenue Estimates

DCMS, and wider government departments aligned to the National Cyber Security Strategy (2016-21) and the Industrial Strategy have sought to promote further understanding of the size and scale of the UK cyber security sector, both at the aggregate level and at the firm level. This has been informed by many research assignments in recent years:

Date	Study / Commissioned / Department	Metrics and Findings
2013	<p>Competitive Analysis of the UK Cyber Security Sector </p> <p>Pierre Audoin Consultants (PAC) </p> <p>Department for Business, Innovation and Skills (now BEIS)</p>	<p>In 2013, BIS commissioned Pierre Audoin Consultants (PAC) to undertake analysis of the UK cyber security sector. PAC estimated that the UK market for cyber security (i.e. the volume of products and services purchased by UK firms to secure their assets) was worth almost £2.8bn in 2013 and projected that the market would be worth £3.4bn by 2017.</p> <p>When defining the cyber security market, PAC identified four submarkets for consideration:</p> <p>Defence and intelligence: this submarket is focused on securing the nation's secrets, and involves the security and intelligence agencies as well as the Ministry of Defence (MoD). It incorporates the most advanced (and most secret) cyber security technologies available. It is, however, a niche market and is relatively constrained in size.</p> <p>Government, other than Defence & Intelligence: this submarket incorporates all the other government funded cyber security tasks without its defence and intelligence obligations. It includes security of health and education data, crime and criminal justice information, as well as more standard (but essential) government operations. Although the requirements of this segment are varied and not as sophisticated as defence and intelligence, the segment is substantially larger in volume and spend.</p> <p>Enterprises: the bulk of the cyber security market is orientated around large commercial enterprises securing their day-to-day business. This would include banks, telecommunications companies, utility and energy firms, manufacturers and retailers, and its constituency comprises the largest firms indigenous to or operating in the UK. Some of these firms have a role to play in the nation's Critical National Infrastructure (CNI), but the nature of the threat is considerably less than that for intelligence and defence organisations.</p> <p>SMEs and consumers: most small and medium-sized businesses have cyber security needs, but these can be substantially less in sophistication and scale to those experienced by larger organisations in government and business. Similarly, consumers do have cyber security requirements but again these tend to be at the lower end. PAC aggregated the submarket for SMEs and consumers because the supply chains serving their needs are viewed as similar.</p>

2013 – 2015	<p>UK Defence and Security Export Statistics</p> <p>kMatrix</p> <p>UK Trade and Investment Defence and Security Organisation (UKTI DSO) (now Department for International Trade Defence and Security Organisation, DIT DSO)</p>	<p>In 2013, kMatrix (a market intelligence provider) were commissioned by UKIT DSO to provide defence and security export statistics. UK defence export performance data is based upon information provided (orders) by hundreds of UK firms to UKTI by survey, in addition to open source access to defence export contracts of other countries.</p> <p>Security sector data was compiled by kMatrix, and includes sales and exports of security equipment and services. Security includes cyber security, and ‘other security’.</p> <p>The methodology utilised by kMatrix to measure sales and exports in cyber security is defined as ‘multi-sourced’ in that it utilises both national statistical data, trade and industry data, and offers a ‘big data’ approach to identifying and measuring economic activities. This is reviewed throughout this section.</p> <p>Key Findings (2015)¹⁴:</p> <ul style="list-style-type: none"> • Cyber Security Exports by UK firms = £1.8bn (45% of all security exports). • Increases in cyber-crime, re-labelling of IT activities as ‘Cyber’, better economic conditions and more proactive responses to cyber defence have all played a part in the strong cyber growth. • kMatrix’s view of the sector (taxonomy) includes: <ul style="list-style-type: none"> – Cyber Consultancy Services – Cyber Infrastructure – First Party Cyber Security Insurance (added in 2014) – Third Party Cyber Security Insurance (added in 2014) – Outsourced/Managed Services – Mobile – Business Continuity – Anti Malware – Application Security – Encryption – Identity & Access Based Services – System Recovery & Data Cleansing – Situational Awareness
2016	UK Defence and Security Export	In 2016 ¹⁵ , DIT DSO commissioned Frost & Sullivan to provide market assessment of the defence and security sectors.

¹⁴ UK Trade & Investment Defence & Security Organisation, *UK Defence & Security Export Statistics for 2015*. (2016). Available at: [https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/541330/20160727 - Official Statistics - UKTI DSO Core Slides for 2015 - Final Version.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/541330/20160727_-_Official_Statistics_-_UKTI_DSO_Core_Slides_for_2015_-_Final_Version.pdf).

¹⁵ UK Trade & Investment Defence & Security Organisation, *UK Defence & Security Export Statistics for 2016*. (2017). Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/631343/UK_defence_and_security_export_s

	<p>Statistics (as above)</p> <p>New Supplier: Frost & Sullivan</p>	<p><i>“The Frost & Sullivan data shows Cyber Security to be the largest single security export category in 2016 at 34%, which was also the position in 2015 even though the figures were accounted for differently.</i></p> <p><i>The UK cyber security exports figure for 2016 is a considerable achievement, £1.5bn, given the competitiveness of the market, but not a surprise given the rise in cyber threats and UK pedigree (more than 70 years’ experience and history of innovation).</i></p> <p><i>It is important to recognise that the figure was generated using a different methodology and taxonomy/segmentation to the previous supplier whose data covered the 2013-2015 period. It cannot therefore be directly compared with previous year’s figures without an appreciation of the accompanying methodology papers that are available on the gov.uk website. This sector is expected to provide the strongest export market growth (12%).”</i></p> <p>The variance in the methodologies deployed by kMatrix and Frost & Sullivan results in a lower 2016 figure for cyber security exports than in 2015.</p> <p>Frost & Sullivan define cyber security (under the HM Government Security Export Growth Strategy (HMG SEGS)) as ‘the products, solutions and services across all industries from Government, CNI and Commercial’, and includes the technology segments of ‘Network Access and Operations’, ‘Analytics and Compliance’, ‘Security Services’, ‘Internet Property Defence’, and ‘Device Management’. However, they recognise limitations in estimating the cyber security sector:</p> <ul style="list-style-type: none"> • The complex nature of the security market makes forecasting a complicated process. Security companies are secretive by nature, and governments and critical infrastructure operators are reluctant to release security budgets, contract awards and operational information. • Visibility on deals and contract awards are often confidential or classified and not in the public domain. • Availability of company data can be limited, especially the percentage of the revenues that are derived from security (especially within large Defence & Security Providers, ICT organisations or services companies.) • The blur between security and defence contracts, especially when militaries are responsible for security operations such as borders or internal counter terrorism. • Complicated nature of what constitutes a security export.
2017	UK Cyber Security Sectoral Analysis	<p>In 2017, RSM Economic Consulting was commissioned by DCMS to undertake a UK Cyber Security Sectoral Analysis. Its key findings were as follows:</p>

	<p>RSM Economic Consulting</p> <p>Department for Digital, Culture, Media and Sport (DCMS)</p>	<ul style="list-style-type: none"> • RSM analysis estimates there are currently 846 firms actively providing cyber security products or services in the UK. • RSM estimate that the cyber security sector's total revenue in FY2015/16 was £5.7bn. • RSM estimate that the cyber security sector's total Gross Value Added (GVA) contribution was £2.3bn in FY2015/16. • RSM estimate there are c. 31,300 – 40,000 staff (FTE) employed in the UK cyber security sector. For transparency, this includes staff within firms providing cyber security products and services, but does not include CISOs, or support staff. • On average, RSM estimate that the sector's revenue per employee in FY2015/16 was £181,000 and GVA per employee was £75,000. • The majority of firms are active in providing Network Security, Information Risk Assessment & Management and Cyber Professional Services. • 89% of the firms are SMEs and collectively drive £1.5bn (26%) of the sector's revenues. The larger firms (11%) earned £4.2bn (74%) in cyber security revenues in FY2015/16. • In the past five years (2012-17), the number of firms active in the sector has grown by over 50%, with over 100 new business registrations in the market within the past two years, representing a surge in new entrants to the market. <p>This exercise sought to review the UK cyber security sector at a detailed and granular level, to ensure an up-to-date economic profile of the sector. This includes the number of UK cyber security companies, the sector's contribution to the UK economy (through revenue and GVA), the number of personnel employed in the sector, and the products and services offered by these firms. This review also explored the investment and funding available to the sector for growth and development, as well as support for training and development and labour supply. Ultimately, this review offers a current baseline¹⁶ for the economic contribution of the UK cyber security sector. It offers an opportunity for the tracking of progress within the sector, and for further evidence to be gathered to identify barriers to growth.</p> <p>In recognition that the UK cyber security sector does not have a formal Standard Industrial Classification (SIC) code, the approach utilised within this study reflects a defined sector utilising a taxonomy developed by DCMS, in collaboration with the National Cyber Security Centre (NCSC), the Department for International Trade (DIT) and RSM.</p> <p>The full RSM methodology is included in Appendix B.</p>
--	---	---

¹⁶ Data is based upon reported 2015/16 financial accounts of UK registered firms.

Revisiting the Sectoral Analysis:

Section 2.5 details analysis undertaken in Spring 2018 to consider the role of:

- The value of internal cyber security functions
- Cyber insurance market

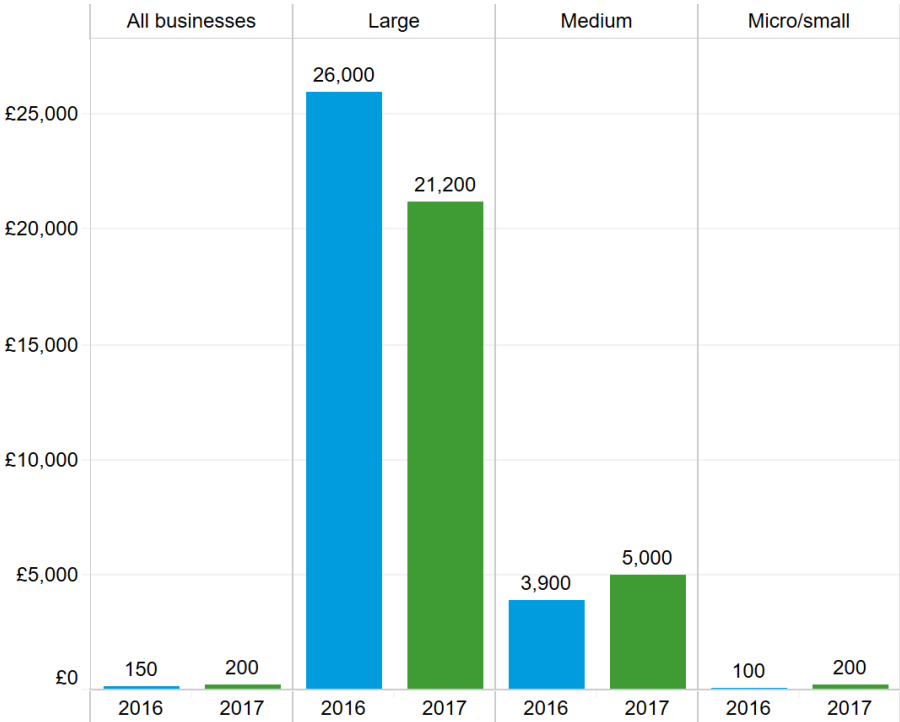
2.5 Additional Cyber Security Related Activity Revenues

As part of this assignment, two areas of economic activity not included in the original RSM UK Cyber Security sectoral analysis were identified for measurement; cyber security insurance and internal functions within companies to employ information security teams. Earlier studies did not include analysis regarding ‘internal expenditure on cyber security functions’.

Each of these inclusions will be explored in detail, providing rationale for potential inclusion in a cyber security taxonomy, and informing economic estimates of these cyber-related activities.

Figure 14 shows that firms have been increasing their typical investment in cyber security in the last financial year between 2016 and 2017, with the exception of medium sized firms.

Figure 14: Median investment in cyber security in the last financial year



Source: Cyber Security Breaches Survey (2017)

Although average costs of cyber breaches have been decreasing over the last two years¹⁷, the cost of non-compliance is arguably rising. With the emergence of GDPR, cyber security practices are changing within firms. According to the 2018 DCMS Cyber Security Breaches Survey, when asked if any changes had been made to cyber security policies regarding the incoming GDPR regulation change, 49% of businesses and 35% of charities said that some of the changes being made, related to their cyber security practices.¹⁸

¹⁷ Ipsos MORI Social Research Institute and University of Portsmouth, *Cyber Security Breaches Survey 2017*. (2017). Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/609186/Cyber_Security_Breaches_Survey_2017_main_report_PUBLIC.pdf

¹⁸ Ipsos MORI Social Research Institute and University of Portsmouth, *Cyber Security Breaches Survey 2018: Preparations for the new Data Protection Act*. (2017). Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/675620/Cyber_Security_Breaches_Survey_2018_-_Preparations_for_the_new_Data_Protection_Act.pdf

Most commonly, this involved updating policies or procedures to be 'in line' with upcoming changes with charities more likely to incorporate software/technology specific changes such as firewall updating, data encryption or outsourcing cyber security.

Although still speculative, the impact of these changes on the nature of cyber-attacks may change. With an increased emphasis from the government to have the correct regulations in place, the penalty of 'non-compliance' is greater than before. The implications are two-fold, as not only would firms face fines and damage to reputation if the GDPR is not followed correctly and an attack occurs, but also competitors with full compliance may have an advantage.

However, understanding this increased 'external' cost associated with the GDPR, an attacker now has increased leverage and has the incentive to demand a larger ransom than before. This increased profitability associated with attacks may adversely signal to more adversaries leading to an increase in the complexity and quantity of attacks. However, in turn this may drive an increased uptake in cyber security protection purchased by firms of all sizes, particularly if it acts as a source of competitive advantage.

Cyber Security Insurance

2.5.1 Defining Cyber Security Insurance



Cyber insurance covers the losses relating to damage to, or loss of information from, IT systems and networks."

Association of British Insurers (ABI)

PwC's 21st Annual Global CEO Survey 2018 identified the most prominent threats facing CEOs in the economic and business environment today. The report highlighted that the speed of technological change is cementing the fear that cyber threats are becoming more frequent and complex in nature. 40% of respondents answered that they are 'extremely concerned' by cyber threats, making the fear of cyber-attacks the fourth most prevalent threat amongst CEOs in the business world.¹⁹

As the threat of cyber-attacks becomes more prominent with recent attacks including the global WannaCry ransomware which affected 99 countries across the world in 2017²⁰, firms globally are beginning to insure their assets in the case of instances such as fraud, malware and a multitude of other cyber security breaches.

According to the Cyber Security Breaches Survey 2017²¹, 46% of all businesses identified at least one cyber security breach or attack in the last 12 months. The attacks were more prominent among large firms, of which 68% experienced a breach or attack, closely followed by 66% of medium firms, 52% of small firms and 38% of micro firms.²² Cyber insurance arguably provides a layer of peace-of-mind in the case of a breach, although the extent of coverage under current cyber risk policies has been a key topic in the industry, given the continually shifting risk landscape.

As with any type of insurance, the policy is tailored to the risk profile of the firm applying, as well as the needs of the firm in question. For example, some firms may require protection against electronic theft of third party confidential information / IP, while the majority would request or expect protection against regulatory investigations and fines in their selected policies.

¹⁹ PwC, 21st CEO Survey. (2018). Available at: <https://www.pwc.com/gx/en/ceo-survey/2018/pwc-ceo-survey-report-2018.pdf>

²⁰ <http://www.bbc.co.uk/news/technology-39901382>

²¹ Ipsos MORI Social Research Institute and University of Portsmouth, *Cyber Security Breaches Survey 2017*. (2017). Available at:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/609186/Cyber_Security_Breaches_Survey_2017_main_report_PUBLIC.pdf

²² The categorisation of firms by size are Large (250+), Medium (50-249), Small (10-49), and Micro (1-9).

This section will set out and explore the following topics in more detail:

- Key insurance providers;
- Requirements of the market;
- Premiums and pay-outs;
- Access to products by firm size;
- Regulatory considerations; and
- Cyber security partnerships with insurance providers

2.5.2 Cyber Security Insurance Providers

The increase in uptake over time for cyber security insurance, as well as increased diversification of products offered has been due to an increase in both complexity and regularity of attacks throughout a variety of markets and organisations ²³.

Insurance providers within the sector, range from large multinational companies (see Figure 1) such as Hiscox, AIG and Chubb (with arms of the business based in the UK) which provide a broader coverage, to smaller exclusively British brokers (see Figure 2) such as Bromwall, Bluefin and K&D which will specialise in covering more niche, cyber security business requirements.

The significant diversity in product offerings within the cyber security insurance market is summarised within a report conducted by Risk Management Solutions (RMS) and the Cambridge Centre for Risk Studies (2016) in which they found that ‘of the insurance products reviewed, almost no two products have the same number and types of coverage in their offering.’²⁴ The cyber insurance market therefore is by its very nature, complex with unique provision at the firm level, given the modelling involved in risk, risk appetite and management.

Figure 15: Multinational Companies



Figure 16: British Companies



²³ Mark Camillo (2017) Cyber risk and the changing role of insurance, Journal of Cyber Policy, 2:1, 53-63, DOI: 10.1080/23738871.2017.1296878. Available at: <https://www.tandfonline.com/doi/full/10.1080/23738871.2017.1296878>

²⁴ Cambridge Centre for Risk Studies-Risk Management Solutions, Inc. *Managing Cyber Insurance Accumulation Risk*. (2016). Available at: https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/risk/downloads/crs-rms-managing-cyber-insurance-accumulation-risk.pdf

2.5.3 Requirements of the Market

The cyber security insurance market is forecasted to grow substantially in the coming decade, with both PwC²⁵ and KPMG²⁶ estimating a total global value of US\$ 7.5 bn by 2020. This would represent a compound annual growth rate of 25% starting from a value of \$2.5bn in 2015, indicating the growing importance businesses and governments alike, are placing on cyber insurance.

PartnerRe's 2016 Survey of Cyber Insurance Market Trends (2016) highlighted that the primary driver for purchasing cyber insurance policies is the news of cyber-related losses experienced by other firms. There have been instances recently, where the cost of data breaches has exceeded £100m in direct and indirect costs, with further impact on brand reputation and loss of customers. This seems to have made the threat seem very real to businesses.

Following the NotPetya ransomware attack in 2017 which affected countries across Europe and the US, Reckitt Benckiser, a global manufacturer which manages brands such as Dettol and Neurofen, lost an estimated £100m in revenue as it experienced disruption to production and deliveries of goods to customers in several countries.²⁷ Such example of a high-cost data breach highlights the potential for organisations to purchase insurance policies as protective measures against the growing threat of cyber-attacks.

The next most common driver for cyber insurance purchases, and one which ties in with upcoming GDPR implementation in May 2018, is that cyber insurance is now required by a third party, such as a customer.

2.5.4 Access to Products by Firm Size

This section evaluates the extent to which different sized firms have access to cyber security risk management services, whether this be the purchase of security solutions such as cloud security and threat detection software, or of cyber risk insurance.

The UK Cyber Security Breaches Survey 2017 highlights the disparities in spending patterns on investment in cyber security by firm size.

Table 3: Cyber Security Breaches Survey Mean and Median Cyber Security Spending by Company Size

	Micro/small (1-49 employees)	Medium (50-249)	Large (250+)
Mean spend	£4,590	£15,500	£387,000
Median spend	£200	£5,000	£21,200
% which spent £0	34%	13%	9%

Source: Cyber Security Breaches Survey (2017)

Although there are no stated direct spending patterns on cyber insurance by firm size within the survey, it is clear there is a prominent gap in the median spend in general security investment between SMEs and large companies; this gap can provide insight into likelihood of spending patterns into cyber insurance. The survey findings also highlight that nearly two-fifths (38%) of firms have insurance covering cyber security breach or attack, although this is not categorised by type of firm.²⁸

²⁵ PwC, *Insurance 2020 & beyond: Reaping the dividends of cyber resilience*. (2015). Available at: <https://www.pwc.com/gx/en/insurance/publications/assets/reaping-dividends-cyber-resilience.pdf>

²⁶ KPMG. *Seizing the cyber insurance opportunity: Rethinking insurers' strategies and structures in the digital age*. (2017). Available at: <https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2017/07/cyber-insurance-report.pdf>

²⁷ The Guardian (2017) 'Cyber Attack - <https://www.theguardian.com/business/2017/jul/06/cyber-attack-nurofen-durex-reckitt-benckiser-petya-ransomware>

²⁸ Ipsos MORI Social Research Institute and University of Portsmouth, *Cyber Security Breaches Survey 2017*. (2017). Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/609186/Cyber_Security_Breaches_Survey

It is likely that those 38% with coverage will fall into the 'large business' category due to their availability of funds. Due to the information held within larger firms, there is a greater likelihood of attack, justifying an enhanced proclivity to invest their funds in securing their IT through implementation of new hardware and software, as well as cyber insurance.

As a result of more limited budget however, SMEs may be less likely to invest significant amounts into cyber insurance, although the need for such services may be increasing.

The looming threat of cyber-attacks has meant larger organisations are demonstrating a concerted effort to augment their cyber security frameworks, investing in more advanced security solutions. This, coupled with a more limited security budget among SMEs has meant that cyber-attacks are potentially 'trickling down' to small and medium sized companies more frequently.

There are measures in place to reduce the premiums paid by companies, which can remove the barriers to entry for smaller firms. As is the case with insurance in any sector, moral hazard plays an issue in the behaviour of firms in protecting their assets through proactive measures.

Insurance providers are circumventing moral hazard issues by offering discounted premiums to firms which have implemented cyber security software solutions; specific to the UK, some SMEs benefit from a Cyber Essentials certification, demonstrating capability in becoming more cyber resilient.

2.5.5 Cyber Security Partnerships with Insurance Providers

There is an argument that cyber security insurance should not sit within the current cyber security taxonomy due to its capacity, or lack thereof, in further providing cyber security solutions to organisations and government, unlike other cyber-related activities currently included within existing taxonomies for the UK cyber security sector.

However, there are instances whereby providers within cyber insurance sector are seeking to minimise their clients, and hence their own, risk exposure to cyber-attacks.

There is evidence within the market that insurance providers have pre-existing relationships with cyber security product providers and consultancies which sit within the cyber security sector. For example, AIG has offered discounts in the past for firms using Invicta Network's security device for shifting Internet Protocol addresses, and Lloyds of London has provided a discount for firms using Tripwire's Integrity security software.²⁹

The cyber insurance sector is actively influencing activity in the broader cyber security sector through these partnerships as it seeks to drive cyber resilience across organisations with reward of cheaper premiums.

Further partnerships have been formed within the sector, including cyber security consultancies which provide governance and management for organisations. As part of their first-party insurance cover, Jardine Lloyd Thompson Group offer claimants the services of consultancies to help manage situations of cyber extortion.³⁰

IASME is an accreditation body which assess and certifies against the Government's Cyber Essentials Scheme. To achieve Cyber Essentials accreditation, a company must implement the steps set out by Government and undergo a live assessment with one of the accreditation bodies. This is costed at £300 plus VAT, which in addition to certification, also provides UK domiciled organisations with less than £20m turnover, automatic cyber liability insurance.

[2017 main report PUBLIC.pdf](#)

²⁹ Gordon, L.A., Loeb, M.P. and Sohail, T., 2003. A framework for using insurance for cyber-risk management. Communications of the ACM, 46(3), pp.81-85. Available at:

http://ns2.dpix.pestiest.hu/~mfelegyhazi/courses/EconSec/readings/09_Gordon2003FrameworkUsingCyberInsurance.pdf

³⁰ JLT (2018) Cyber Insurance, Available at: <https://www.jltspecialty.com/what-we-do/insurance-risks/cyber-risks/cyber-insurance-1st-party>

In addition to the core cyber security benefits resulting from the scheme, companies are receiving cyber insurance coverage, thus providing further evidence of the link between cyber insurance and other cyber-related activities.

2.5.6 Quantification of the Cyber Insurance Market

With cyber security being a relatively unexplored market within the UK, there is little consensus as to the value of the sector, or indeed the associated insurance sector. As such, to derive an estimated figure for the UK a variety of sources and methods are used in this section to produce a range within which a benchmark estimate lies.

Benchmark studies

Due to the relatively embryonic state of the cyber security sector, few studies have been commissioned to provide estimates of the UK cyber sector, and consequently, there has been limited opportunity to quantify the UK cyber insurance sector.

In 2016, Frost & Sullivan underwent an exercise to quantify the UK defence and security exports, utilising a method aligned to HMG Security Export Growth Strategy (SEGS) Capability Areas, of which includes a cyber insurance segment. In 2013, Pierre Audoin Consultants were commissioned by the Department for Business, Innovation and Skills to complete a competitive analysis of the UK cyber security sector. Within this, the report suggests that there was opportunity for UK-based insurance companies to take a lead in offering insurance products to insure against cyber breaches. More importantly, and set out in Section 2.1.7, insurance providers could begin to develop partnerships with businesses offering cyber security products as part of a method to offer cheaper premiums to end customers.

Table 4: existing cyber security insurance estimates and implications

Data Points	Source	Information	Limitations	Average
Global insurance market value	Allianz ³¹ , Ernst & Young ³²	Allianz and Ernst & Young provided data for the gross written premiums written by insurers globally. Data for Allianz was provided in EUR, to convert to USD an exchange rate of 1.24 was used. The data is sourced from 2015.	The data provided does not account for 'newer' developments within the cyber security insurance market which will impact the overall insurance market. Furthermore, the values may have been different at the time of publication, with a varied exchange rate.	US\$4.42tn
Global cyber insurance market value	Advisen ³³ , Allianz ³⁴ , AON, KPMG ³⁵ ,	Various consulting firms and analysis centres had conducted studies, valuing the gross written premiums for cyber security insurance	The data provided does not account for any of the most recent developments which may lead to an increase in demand for insurance, such as the GDPR policy in the UK or recent	\$2.45bn

³¹ Allianz (2016) 'Global Insurance Markets – Current Status & Outlook up to 2026':

https://www.allianz.com/v_1462226400000/media/economic_research/publications/working_papers/en/GVM26Apr2016e.pdf

³² EY (2016) 'Global Insurance Trends Analysis 2016': [http://www.ey.com/Publication/vwLUAssets/ey-global-insurance-trends-analysis-2016/\\$File/ey-global-insurance-trends-analysis-2016.pdf](http://www.ey.com/Publication/vwLUAssets/ey-global-insurance-trends-analysis-2016/$File/ey-global-insurance-trends-analysis-2016.pdf)

³³ Advisen (2016) '2016 Survey of Cyber Insurance Market Trends' <https://www.advisenltd.com/wp-content/uploads/2016/10/cyber-insurance-market-trends-paper-2016-10-24.pdf>

³⁴ Allianz (2015) 'Cyber Risk 2025 – the next ten years': <http://www.agcs.allianz.com/insights/expert-risk-articles/cyber-risk-2025/>

³⁵ KPMG (2017) 'Seizing the cyber insurance opportunity: Rethinking insurers' strategies and structures in the digital age' <https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2017/07/cyber-insurance-report.pdf>

	Lloyds ³⁶ , PwC, S&P	in 2015. These ranged from \$1.7bn to \$3.5bn.	attacks such as 'WannaCry'. Recent attacks would also have led to an increase in the values of premiums issued, globally.	
Cyber security insurance as a percentage of the global insurance market	Deloitte ³⁷	Deloitte stated that \$1.5bn of premiums issued in the USA were cyber related, from a total of \$508bn gross written premiums. This provided a fraction which was used as a proxy for 'global' cyber premiums as a percentage of the total insurance market.	This is a very crude measure and only accounts for the US market meaning its scalability to other markets is dubious.	0.3%
UK insurance market value	Hiscox ³⁸	Hiscox estimated the value for gross written premiums in the UK for 2016.	The data provided does not account for 'newer' developments within the cyber security insurance market which will impact the overall insurance market for the UK. Especially considering the UK is one of the key growth markets for cyber insurance since 2017.	\$2.4bn
UK cyber security insurance market value	Marsh ³⁹	Marsh provided a value for the UK cyber insurance market based on the gross value of written premiums.	The data provided does not account for 'newer' developments within the cyber security insurance market which will impact the overall insurance market. Furthermore, the values may have been different at the time of publication, with a varied exchange rate.	\$224 m
UK insurance as a percentage of global insurance	Ernst & Young ⁴⁰	Ernst & Young (EY) provided an estimate for the UK insurance market penetration as a percentage of the global insurance market in 2016, in terms of gross written premiums.	The data provided does not account for 'newer' developments within the cyber security insurance market which will impact the overall insurance market for the UK. Especially considering the UK is one of the key growth markets for cyber insurance since 2017.	10%

³⁶ Lloyds (2017) <https://www.lloyds.com/news-and-risk-insight/press-releases/2017/07/cyber-attack-report>

³⁷ Deloitte: 'Demystifying cyber insurance coverage: Clearing obstacles in a problematic but promising growth market' Available: <https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/financial-services/deloitte-nl-fsi-demystifying-cyber-insurance-coverage-report.pdf>

³⁸ Hiscox (2016) Report and Accounts, Annual Report 2016: https://www.hiscoxgroup.com/sites/group/files/2018-03/Hiscox_report_and_accounts_2016.pdf

³⁹ Marsh & UK Government (2015) UK Cyber Security: The Role of Insurance in Managing and Mitigating the Risk' Available at: <https://www.marsh.com/content/dam/marsh/Documents/PDF/UK-en/UK%20Cyber%20Security%20The%20Role%20of%20Insurance%20in%20Managing%20and%20Mitigating%20the%20Risk-03-2015.pdf>

⁴⁰ EY, See Source 32

UK cyber security market as a percentage of global cyber security market	Marsh ⁴¹	Marsh provides figures for the UK stating that 10% of global cyber insurance in from London. The data is for 2015.	The data provided does not account for 'newer' developments within the cyber security insurance market which will impact the overall insurance market for the UK. Furthermore, this value may not necessarily represent the whole of the UK, it is assumed here that most insurance premiums are purchased within London.	10%
--	---------------------	--	---	-----

These enable provision of a high-level estimate of the UK cyber insurance industry. However, it is worth noting that this should not necessarily be taken as 'additional' to existing estimates. Cyber insurance provides financial cover for firms in the event of loss which can be used to purchase cyber security products and solutions. To include cyber insurance as a value runs potential risk of double counting and over-estimation of the core product and service market. For example, typically car and health insurance would not be included in the sector estimates of the revenues of those industries. This is because the insurance acts as a sector enabler and catalyst for actual expenditure within the sector.

To estimate the UK cyber insurance sector, a range of data was collated from sources such as Allianz, Ernst & Young, PwC and other firms. In total, fourteen data sources were used to derive information for the data points outlined.

This data was then averaged, and varying approaches were developed which provided a range of values for the cyber security insurance market in the UK. **It should be noted that all preceding values for insurance market values are based on premiums, i.e. the cost to business for purchasing a cyber risk insurance policy.**

This has produced an RSM estimate for the scale of the UK cyber security insurance premiums at \$245 million (c. £180m) and draws upon the average global cyber security insurance market from seven sources (US\$ 2.45bn), and desk research (Hiscox, Marsh) that suggests the UK has a global market share of 10% (with the US as a globally mature market with >80% global share).

⁴¹ Marsh, see source 39

Internal Spending

The table below highlights the difference in cyber security investment between 2016 and 2017, as reported by the DCMS Cyber Breaches Survey. Generally, the data shows a marked increase in cyber security spending, with mean spending rising by £530 compared with 2016 across all businesses.

Table 5: Cyber Security Breaches Survey 2017 Changes in Mean and Median Spending by Company Size

	All businesses	Micro/small	Medium	Large
Change in mean spend (£)	+£530	+£310	-£8600	+£118,000
Change in median spend (£)	+£50	+£100	+£1100	-£4800
Change in % spending £0	1%	2%	3%	3%

Source: Cyber Security Breaches Survey (2017)

The developing 'weapons of attack' used by cyber attackers are continuously changing, and the costs are moving at a similar pace. These are become pressing issues which organisations across the public and private sector are now required to deal with more regular than in the last few years.

Table 6: Cyber Security Breaches Survey 2017 Median Number of Cyber Attacks (2016-2017)

Median Number of Attacks	2016	2017
Overall	24	46 (+92%)
Micro firms	17	38 (+124%)
Small firms	33	52 (+58%)
Medium firms	51	66 (+29%)
Large firms	65	68 (+5%)

Source: Cyber Security Breaches Survey (2017)

The likelihood of threats is amplified further by the rising tendency for companies to outsource a plethora of functions to third-party organisations. As third-parties become more efficient in their specialist functions, organisations are attracted to reduced costs and peace-of-mind in outsourcing functions such as HR or finance to third-parties.⁴²

This has created an argument for having an in-house cyber security specialist or team, depending on the size of the company. In-house specialists whom are aware of the risks of data transfer and compliance with GDPR, may be better suited to identify issues with this potential risk and can provide direction and updates to senior-level management staff.

Further to this, the immediacy in which security breaches are required to be dealt with means organisations will either require a third-party which is able to resolve issues quickly, normally within a few hours of the attack, or an in-house team to investigate and rectify the problem. Having an IT specialist in-house also provides a point of contact for other employees in the case of computer bugs or access requests. The intended result is a streamlined and efficient process.

Organisations need to bear in mind however that adversaries are becoming more skilled in their attacks, as phishing emails are beginning to be tailored to individual organisations, while vulnerabilities in networks and systems are being exposed by a growing community of attackers. As the attack perimeter expands, it is

⁴² Elatt (2018) 'Why bring cyber security in house?' Available at: <https://www.elatt.org.uk/news/cyber-security-in-house>

unlikely that organisations, particularly micro or small (1-49 employees) firms with a limited cyber security budget, will be able to source a well-equipped IT security professional which can 'do it all'.⁴³

This section will explore the following topics further:

- What are firms spending?
- Cyber security spending trends
- Quantifying the value of internal cyber security functions within organisations

2.5.7 What are Firms Spending?

On average, security budgets for firms may lie somewhere in the region of 21% of overall IT budgets (excluding headcount).⁴⁴ The Cyber Security trends report (2017) found that the top three security investment priorities for firms in 2018 are cloud infrastructure, cloud applications, and managed security services. Other priorities include; mobile devices, desktops, and laptops.

Based on a US survey of over 1900 organisations that use both in-house and outsourced security, approximately 40% spend between 1-15% on managed security service providers, 50% spend between 16-50% of their budget on outsourced security service providers, and roughly 10% of companies spend over 50% of their IT spending budget on outsourced security services.⁴⁵

2.5.8 Cyber Security Spending Trends

Most of the organisations surveyed in the SANS Institute IT security spending trends (2016) report are spending on access and authentication, advanced malware prevention, and endpoint security tools and technologies, with the main reasons for spending being protection of sensitive data, regulatory compliance, and reducing incidents and breaches.⁴⁶

IT budgets

The SANS paper defines the size of company by number of employees. A small company has less than 500 employees, medium-sized has between 500 and 5000 employees and a large firm have over 5000 employees. (This is not the same as UK / EU definitions for company size).

The table below details spending by company size in 2015:

Table 7: SANS Institute IT and Security Budget by Company Size (2016)

Company size	IT Budget	% Budget for security
Small	\$100k - \$500k	4% - 6%
Medium	\$1M	4% - 6%
Large	\$1M - \$10M	4% - 6%

Source: SANS Survey February 2016, n=169

⁴³ TMCS (2016) ' Outsourcing vs In-House IT': Available at; <http://www.tmcs.co.uk/2016/10/04/outsourcing-vs-in-house-it-the-good-the-bad-the-ugly/>

⁴⁴ ISC², *Cybersecurity Trends Spotlight Report*, (2017). Available at: <https://www.herjavecgroup.com/wp-content/uploads/2017/06/Cybersecurity-trends-2017-survey-report.pdf>.

⁴⁵ Ibid.

⁴⁶ SANS Institute, *IT Security Spending Trends*. (2016). Available at: <https://www.sans.org/reading-room/whitepapers/analyst/security-spending-trends-36697>

In-house spending

According to the SANS report, US firms are not resistant to using in-house staff to facilitate their IT security needs, with nearly half of respondents indicating they allocate more than 11% of their IT security budgets to in-house staff. Only 8% of respondents aren't using any in-house staff whatsoever.⁴⁷

2.5.9 Estimating the value of cyber security functions within organisations

RSM has used a mixture of Office for National Statistics (ONS) Business Count Data, findings from the UK Cyber Security Breaches Survey 2017, and a desk review to find an exhaustive list of out-sourcing estimates as a percent of IT budgets.

Desk Review

RSM completed a desk review of available literature and research papers to collate estimates of the proportion of IT budget expenditure allocated to in-house employees.

Understandably, existing IT budget spending patterns are becoming outdated as firms begin to adjust their IT spending habits. Due to limited estimates for in-house apportionment as a percent of total IT budget, we have collected the percent of IT budgets which are outsourced where possible to inform understanding of IT budgetary allocations.

RSM has identified the following estimates for outsourced IT budgets and outsourced IT security budgets:

Table 8: Existing estimates of outsourced IT budgets and outsourced IT security budgets

Source	% of IT budget spent		% of cyber security budget		Year of estimate	Notes
	Outsourced	In-house	Outsourced	In-house		
Deloitte ⁴⁸	26%	74%			2014	Survey respondents highlighted 26% of IT capabilities are outsourced
Computer economics ⁴⁹	11.9%	88.1%			2017	Survey respondents highlighted 11.9% of IT capabilities are outsourced
PwC ⁵⁰			33%	67%	2017	Cyber security outsourcing as a percent of total cyber security spend is 33%
Alert Logic ⁵¹			22.87%	77.13%	2017	Cyber security outsourcing as a percent of total cyber security budget is 22.87%
Average		81.05%		72.07%		

⁴⁷ ibid

⁴⁸ Deloitte, *Deloitte's 2016 Global Outsourcing Survey*. (2016). Available at:

<https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/operations/deloitte-nl-s&o-global-outsourcing-survey.pdf>

⁴⁹ Computer Economics, *IIT Outsourcing Statistics 2017-2018*. (2017). Available at:

<https://www.computereconomics.com/temp/outsourcingstatistics/samplepages.pdf>

⁵⁰ PwC, *Cyber Security: European Emerging Market Leaders*. (2017). Available at:

<https://www.pwc.co.uk/deals/assets/cyber-security-european-emerging-market-leaders.pdf>

⁵¹ AlertLogic, *Cyber Security Trends: 2017 Spotlight Report*. (2017). Available at:

https://www.ipexpo.eu/content/download/10655/148475/file/2017_Cybersecurity%20%20Trends_Alert_Logic.pdf

Based on the estimates for outsourcing, we can assume that the remaining IT budget is apportioned to in-house personnel, as well as software and hardware purchases. Unfortunately, deeper analysis of this apportionment has not been published, and as a result, we allocate the remaining budget to in-house spending.

It should be noted that realistically, there will be some allocation to software and hardware purchases, which would be covered under RSM's original Cyber Security Sectoral Analysis completed in 2017. Double-counting should therefore be considered and mitigated.

Gartner IT and Cyber Security Expenditure:

Regarding absolute values in IT and cyber security budget and expenditure within firms, Gartner (2016)⁵² has also identified that global IT spending (including internal and external functions) reached \$3.41tn in 2016, of which 5.3% is within the UK.

Based on an average 2016 exchange rate of £1.36: £1 (XE), IT budgets across all sectors in the UK are estimated at £132.9bn per annum (an average of £23,000 per active UK business).⁵³

Gartner also provide a breakdown on IT security spending as a percentage of IT budgets. They note the difficulty in estimating this figure as many firms find it challenging to proportion their IT budget into subcategories e.g. security may be an 'in-built' component of a contract, rather than a direct purchase. As a result, they estimate that IT security spending as a percentage of business IT budgets ranges from 1 – 13%, but on average is 5.6% (for every £1,000 of IT budget, a firm can be expected to spend approximately £56).

This provides an estimated average cyber security budget for UK firms of £1,306 annually, and total cyber security budgets of £7.4bn per annum.

⁵² Gartner (2016) 'Gartner Says Many Organizations Falsely Equate IT Security Spending With Maturity' Available at: <https://www.gartner.com/newsroom/id/3539117>

⁵³ Total UK expenditure (IT Budgets) = £132.9bn / 5,694,515 businesses (BEIS 2017 UK Population Estimates).

The UK Cyber Security Breaches Survey 2017

The Cyber Security Breaches Survey 2017 targeted a population which matched that of its 2016 Survey, the purpose of which was to provide deeper insight into the extent to which UK businesses approach cyber security, and the level, nature, and impact of cyber-attacks on businesses.

The sample frame was the Government's Inter-Departmental Business Register (IDBR), which covers businesses in all sectors across the UK at the enterprise level, which is the main sample frame for Government surveys of businesses and for compiling national statistics.

The target population included:

- private companies with more than one person on the payroll
- charitable companies and non-profit organisations
- universities and independent schools or colleges

The focus of the survey was to provide evidence on businesses' engagement, to inform future policy for this audience. Public sector organisations (Standard Industrial Classification, or SIC, 2007 category O (84)) were therefore considered outside of the scope of the survey and excluded from the sample selection.

Organisations in the agriculture, forestry and fishing sectors, as well as those in the mining and quarrying sectors (SIC, 2007 categories A (01-03) and B (05-09)) were also excluded.

RSM have used findings from the Survey to identify key spending patterns by business in the UK to protect against cyber risk and should serve as applicable and robust values for estimating the value of internal cyber security functions within organisations.

Respondents were asked to include any spending on any activities or projects to prevent or identify cyber security breaches or attacks, including software, hardware, staff salaries, outsourcing and training-related expenses. These are as follows:

Table 9: Cyber Security Breaches Survey 2017 Average Investment in Cyber Security in Last Financial Year

	All businesses	Micro/small	Medium	Large
Median Spend	£200	£200	£5,000	£21,200
Base	1,209	829	268	112
% of firms spending £0		34%	13%	9%

Source: Cyber Security Breaches Survey 2017

It should be noted that the Survey has categorised businesses by employee size as follows: Micro (1-9); Small (10-49); Medium (50-249); Large (250+).

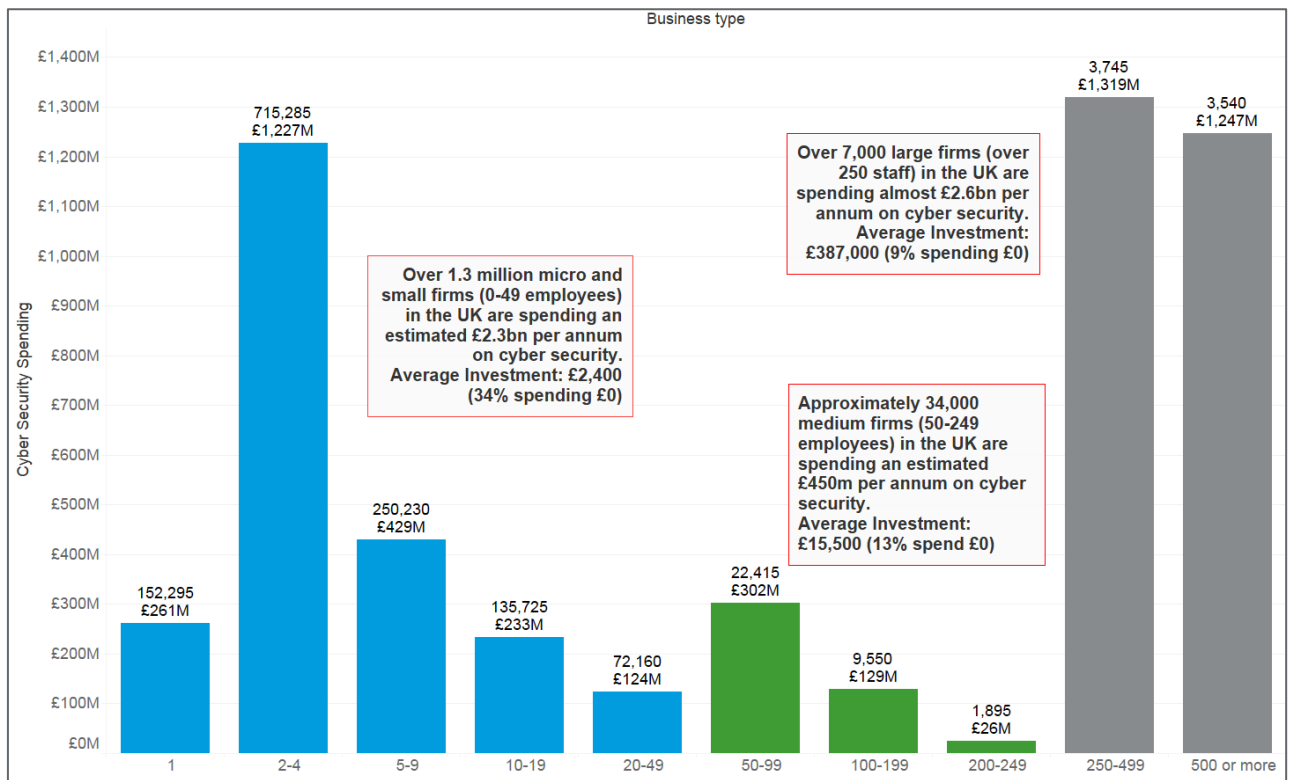
Table 10: RSM analysis of internal spending on cyber security functions

Number of Employees	Number of Businesses	Number of Employees (000s)	Turnover (£m)	Estimated Cyber Security Spending	Rationale (based upon Cyber Breaches)
With no employees (unregistered) ²	3,131,285	3,402	111,673	£0	Cyber Breaches 2017: Assume No Spend ⁵⁴
With no employees (registered) ²	1,196,390	1,295	159,901	£0	
1	152,295	339	26,680	£261,338,220	Cyber Breaches 2017: Assume 34% No Spend, 66% Mean Spend £2,600 for Micro/Small
2-4	715,285	2,044	298,614	£1,227,429,060	
5-9	250,230	1,710	227,344	£429,394,680	
10-19	135,725	1,866	229,056	£232,904,100	
20-49	72,160	2,193	310,729	£123,826,560	
50-99	22,415	1,547	230,202	£302,266,275	Cyber Breaches 2017: Assume 13% No Spend, 87% Mean £15,500
100-199	9,550	1,327	238,062	£128,781,750	
200-249	1,895	423	72,652	£25,554,075	
250-499	3,745	1,300	234,643	£1,318,876,650	Cyber Breaches 2017: Assume 9% No Spend, 91% Mean £387,000
500 or more	3,540	9,276	1,599,616	£1,246,681,800	
	1,366,840	22,025	3,467,598	£5,297,053,170	Cyber Breaches Estimate of Cyber Spend
Spending Per Business				£3,875.40	
Spending Per Employee				£240.50	

Source: BEIS Business Population (2017) / Cyber Security Breaches Survey (2017) / RSM (2018)

⁵⁴ It should be noted that due to the limited budgets of micro and small businesses, in addition to their relatively small workforce, we have assumed that any spending, as limited as it may be (median £200), is unlikely to be used on in-house IT security specialists, and will more likely be allocated to IT software such as anti-malware.

Figure 17: Cyber Security Spending by Company Size



2.5.10 Segmenting Security Spending: Emerging Findings

This analysis provides a range of estimates of total spending on cyber security by UK firms (£5.3bn using the Cyber Breaches Survey to £7.4bn (Gartner).

This is not the same as revenue reported by UK cyber security firms (£5.7bn) as this will include revenue from UK firms and exports (and is based upon reported revenue and assumed segmentation, rather than modelling).

However, this provides potential further insight for the Department, as it demonstrates economic activity in the cyber security sector across four areas, namely:

- **Total Domestic Expenditure on Cyber Security: £5.3bn ~ £7.4bn assumed minimum spending.** This is likely to be higher as these estimates are focused at the business level, and may not include public and organisation expenditure. This includes internal and external expenditure.
- **Total Revenue from UK Cyber Security Firms: £5.7bn** – This will include spending by UK firms as captured in the above, but also export sales.
- **Export Revenue in Cyber Security: £1.5bn - £2bn** estimated. This means that it is assumed that approximately 25% of UK cyber security firm revenue is attained through exports, and 75% reflects domestic sales.
- The domestic sales may reflect ‘external’ spending by UK firms e.g. with dedicated firms. This means that £3.7bn - £4.2bn may be a realistic estimate of UK business procurement of cyber security products and services.
- This leaves an estimated **£1.1bn - £3.7bn (assumed mid-point of £2.4bn) of ‘internal expenditure’ by firms in cyber security** e.g. on CISO functions, primarily driven by medium and larger firms.
- RSM estimate the **cyber insurance market** to relatively limited in the UK (**approx. £180m** in 2015; however, this could be set to grow considerably in the next five years with a global market share of c. 10%).

2.6 Gross Value Added

2.6.1 Cyber Security GVA

Gross Value Added (GVA) is a key indicator of the productivity of cyber security firms and of total contribution to the economy. GVA is driven primarily by a firm's gross profit and employee remuneration; therefore, an increase in GVA can also indicate improved economic health in a sector, as well as signpost to a sector with a wage premium.

In the most recent available year (2015/16), cyber security GVA within the sector (846 firms) is estimated at £2,349,347,289 (£2.3bn to the nearest £100m).

For analysis purposes, each firm's cyber security employment percentage of overall employment is expected to hold for GVA, e.g. where 60% of staff are working in cyber security, it is assumed 60% of the firm's GVA comes from cyber security activity⁵⁵. Therefore, the total estimated GVA figure of £2.3bn is representative of the cyber security activity of firms only.

The GVA to turnover ratio across all firms (n=846) is 0.41 (turnover to GVA ratio of 2.4). This means that for every £1 the cyber security sector generates in revenue, 41p in direct GVA is generated. This reflects a GVA to turnover ratio of 0.41⁵⁶. This also means that the average GVA per employee (n=31,339) is estimated at £74,965.

For transparency, this analysis also recognises that existing DCMS Economic Estimates of the Digital Sector in the UK estimate GVA per employee at approximately £84,500⁵⁷.

2.6.2 By Company size category & by dedicated/diversified

Figure 18 provides a breakdown of estimated revenue and GVA by size of firm, and Figure 19 provides these by 'dedicated and diversified'.

Figure 19 demonstrates that dedicated firms have a higher GVA-to-turnover ratio (0.48) than diversified firms (0.38). This provides insight that firms dedicated to cyber security products and services may either be: more profitable (i.e. higher gross profit as a percentage of revenue); have higher remuneration rates; or both than firms which provide cyber security as one of a diversified range of activities.

⁵⁵ This has been tested and validated in the RSM online survey of cyber security firms where estimated % of firm employment and firm revenue 'as cyber' are comparable.

⁵⁶ The figure of 0.41 compares to the UK aggregate value of 0.34 (total turnover to aGVA at basic prices, 2015, Annual Business Survey, ONS).

⁵⁷ Based upon a 2014 estimate of Digital Sector GVA of £118.3bn and 1.4m employed (see DCMS, *Digital Sector Economic Estimates*. 2016. Available at:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/503666/Digital_Sector_Economic_Estimates_-_January_2016_Revised.pdf)

Figure 18 Revenue & GVA (2015/16) by Size

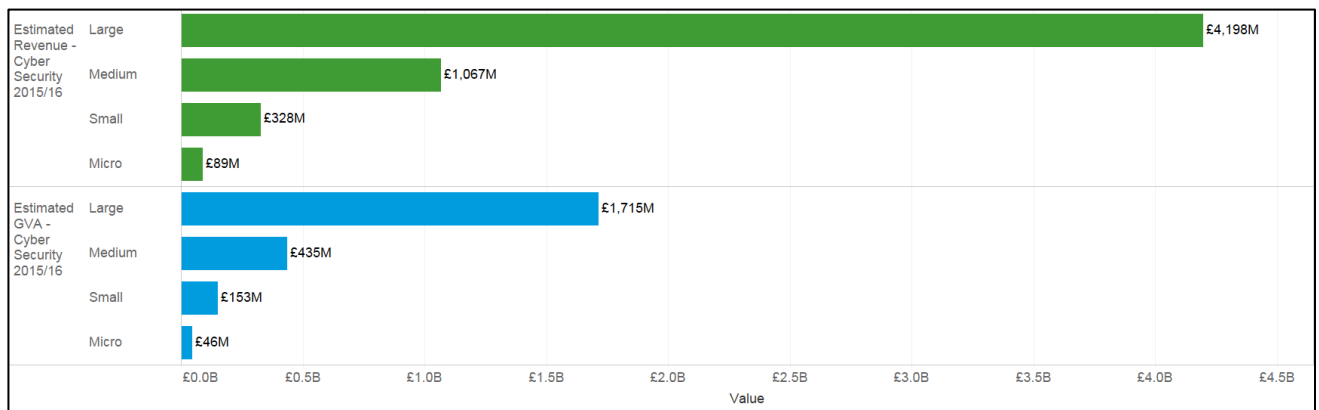
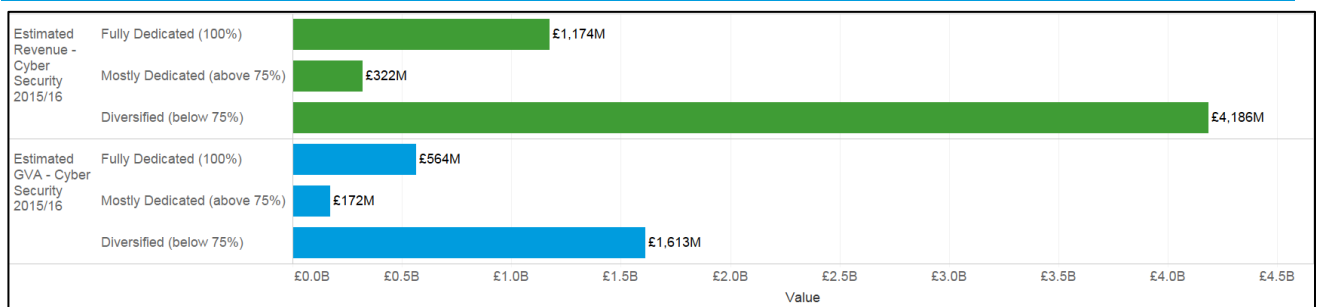


Figure 19 Revenue & GVA (2015/16) by Dedicated/Diversified



Source: BvD, Orbis, RSM Tracker (August 2017)

Figures 20 and 21 set out median and average GVA by size of firm.

Figure 20 Median GVA by Size of Firm (per firm)

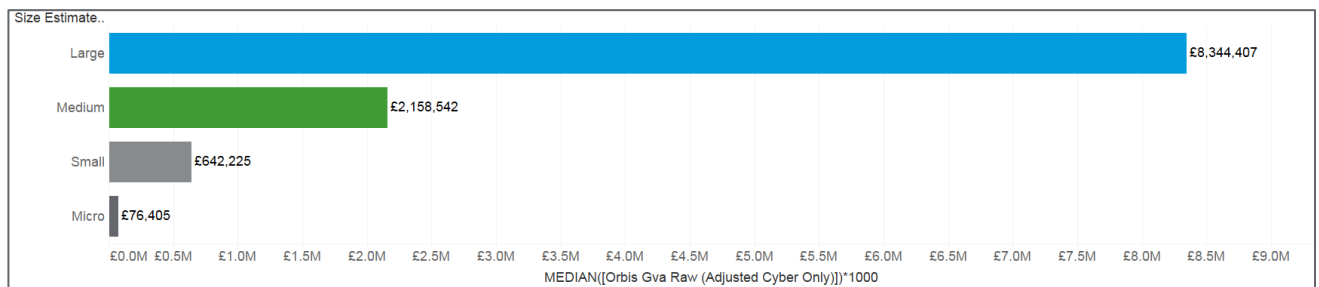
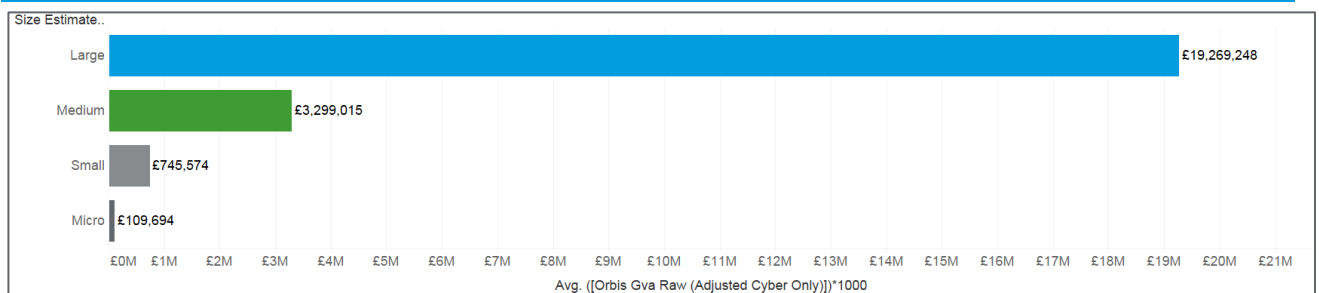


Figure 21 Average GVA by Size of Firm (per firm)



Source: BvD, Orbis, RSM Tracker (August 2017)

2.6.3 GVA per employee

Table 11 provides further insight into the productivity of employees within cyber security by size of firm. Overall, larger firms tend to be more productive than SMEs with regard to GVA per employee.

For SMEs, the GVA per employee estimates show that they have lower values than large firms, given typically lower revenue and profitability per employee. This might suggest that some of these firms may face a greater challenge regarding gross profitability and / or capacity to remunerate staff well in a competitive market, particularly as revenue per employee is much lower in micro and small firms compared to large and medium firms.

This should be an area of continued interest for the Department in tracking the productivity and GVA of smaller firms, and examining the change over time in employment, remuneration, GVA and profitability by type of firm.

Table 11: Estimated GVA per Employee by Size of Firm

	Count	Estimated Revenue by Size	Estimated GVA by Size	Estimated Cyber Security Employment	Estimated Revenue per Employee	Estimated GVA per Employee
Large	89	£4,197,673,387	£1,714,963,109	19,486	£215,420	£88,010
Medium	132	£1,066,625,313	£435,470,039	6,776	£157,412	£64,267
Small	205	£328,448,253	£152,842,742	3,814	£86,111	£40,072
Micro	420	£88,983,771	£46,071,399	1,263	£70,454	£36,478
Grand Total	846	£5,681,730,723	£2,349,347,289	31,339	£181,298	£74,965

Source: BvD, Orbis, RSM Tracker (August 2017)

2.7 Investment Landscape

2.7.1 Introduction

Investment in firms, and access to suitable financing for growth is of key importance to the UK cyber security sector. For the 846 firms identified in this analysis, these have been input into a data platform called Beauhurst (www.beauhurst.com) which tracks announced and private investments in high-growth companies.

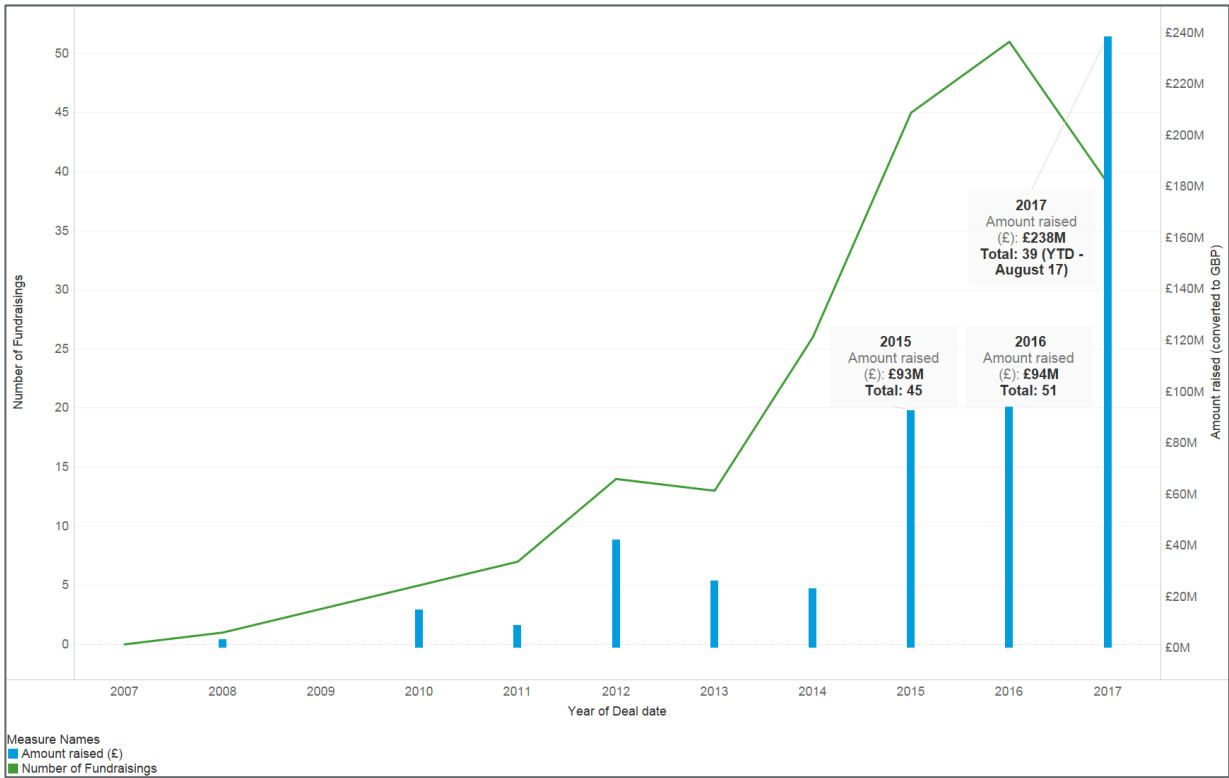
This has identified the firms which have received a tracked investment in the UK, and our analysis is based upon 201 investments identified since 2007⁵⁸ in 84 firms which match the list of firms used in RSM analysis. This is therefore a sample based on known investment and aligns to the taxonomy used to define the sector within this analysis. This chapter should therefore be considered representative of the cyber security sector’s investment performance; however, further analysis would be required to fully ascertain purpose of each investment, relevant investor and investment outcome.

2.7.2 Investments to Date

Through inputting all 846 firms into Beauhurst, this has yielded 201 investments across 84 firms since 2007.

- **Total Fundraising:** £544m
- **Average Fundraising:** £2.7m
- **Median Fundraising:** £432,000
- **Range:** £15,000 - £80m

Figure 22 Investment Timeline



Source: Beauhurst (September 2017)

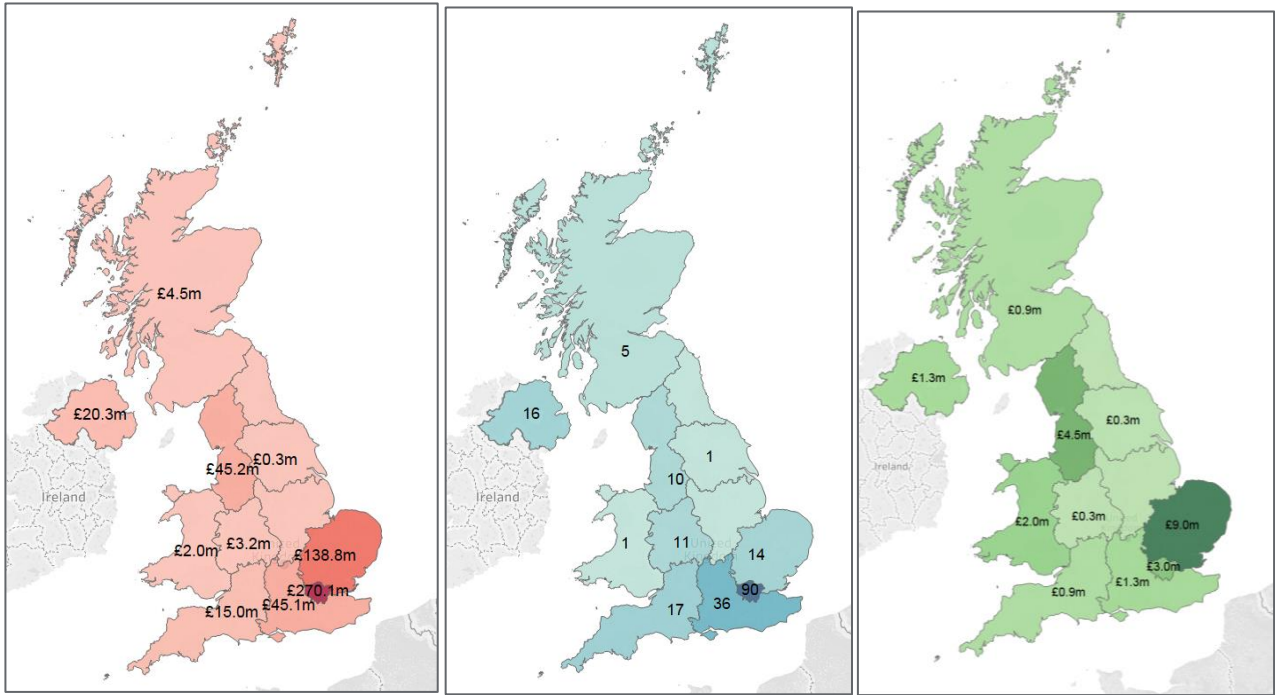
⁵⁸ Please note that Beauhurst coverage is comprehensive since 2011. Beauhurst only have investment data pre-2011 where the company also received investment post-2011.

2.7.3 Investment by Location

Figure 23 sets out the total volume of investment (£) and the number of investments identified within the Beauhurst dataset for cyber security firms. Greater London has the highest total investment (£270.1m) and the highest number of deals (90), with an average investment of £3m per deal. However, the South East has also performed well, with an average investment of £9.9m driven by large scale investments in firms such as Darktrace.

The investment landscape in the North East, Yorkshire and the Humber and East of England is less pronounced, with little investment (regarding number and or value of investments) identified. This signals that investment may be coming through in areas where there has been a concerted effort to increase business scale-up and growth such as in London (CyLon), West Midlands/South West (28 investments in total, adjacent to strong community in Cheltenham), and the devolved regions.

Figure 23 Volume of Investment (Left) and Number of Investments (Centre) and Average Investment (Right) by Region

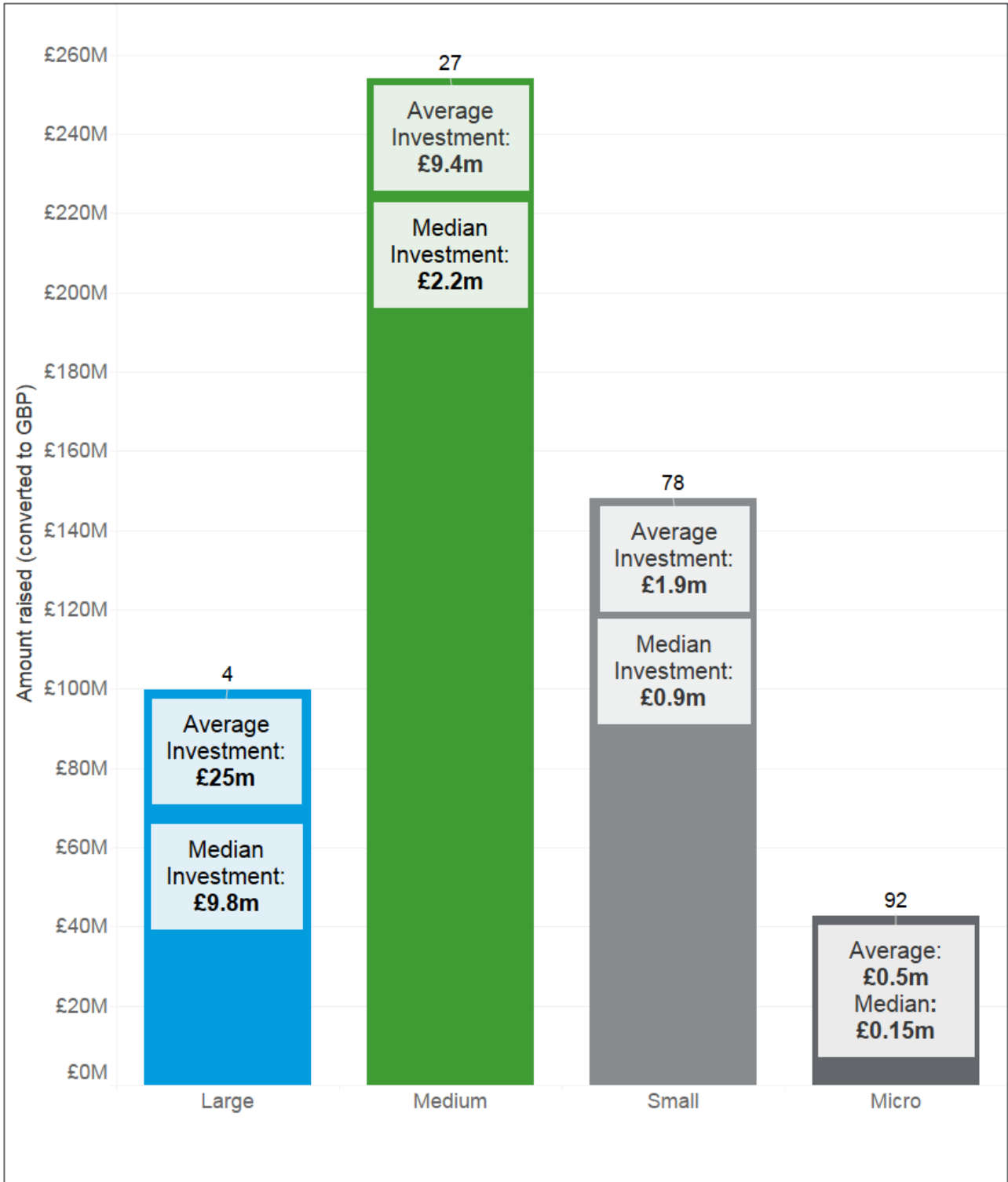


Source: Beauhurst (September 2017)

2.7.4 By Company size category

As noted, the average investment is approximately £2.7m, and the median investment is approximately £430,000 across the UK. There is therefore a wide range of investment values identified within the sector (from £15,000 to £80,000,000) given the varied size of firms. Figure 24 provides an overview of the average and median investments (n=201 deals, noted at the top of each column) by company size.

Figure 24 Average and Median Investment by Company Size



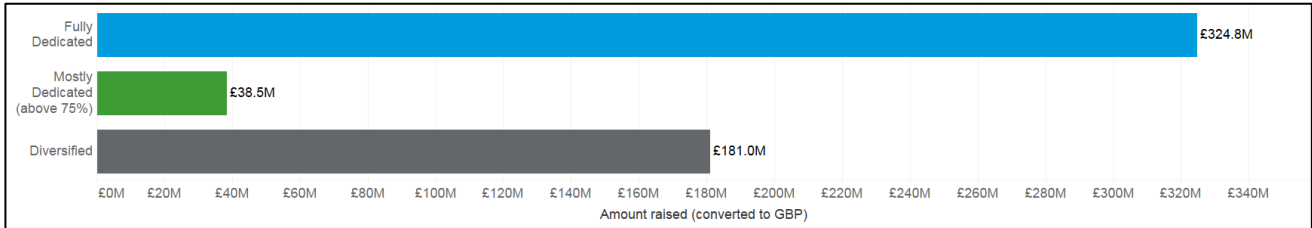
Source: Beauhurst (September 2017)

2.7.5 By Dedicated and Diversified

Figure 25 sets out the identified investment amount by dedicated (where we have reported full employment/revenue to come from cyber security activities), and by diversified (less than 75%).

This provides that almost two-thirds of identified investment is in dedicated firms, which means that the investment data through Beauhurst can be viewed as representative of not only investment in firms which provide cyber security, but also in firms where the majority of their activities (and investments) are linked to providing these products and services.

Figure 25 Investment by Dedicated / Diversified

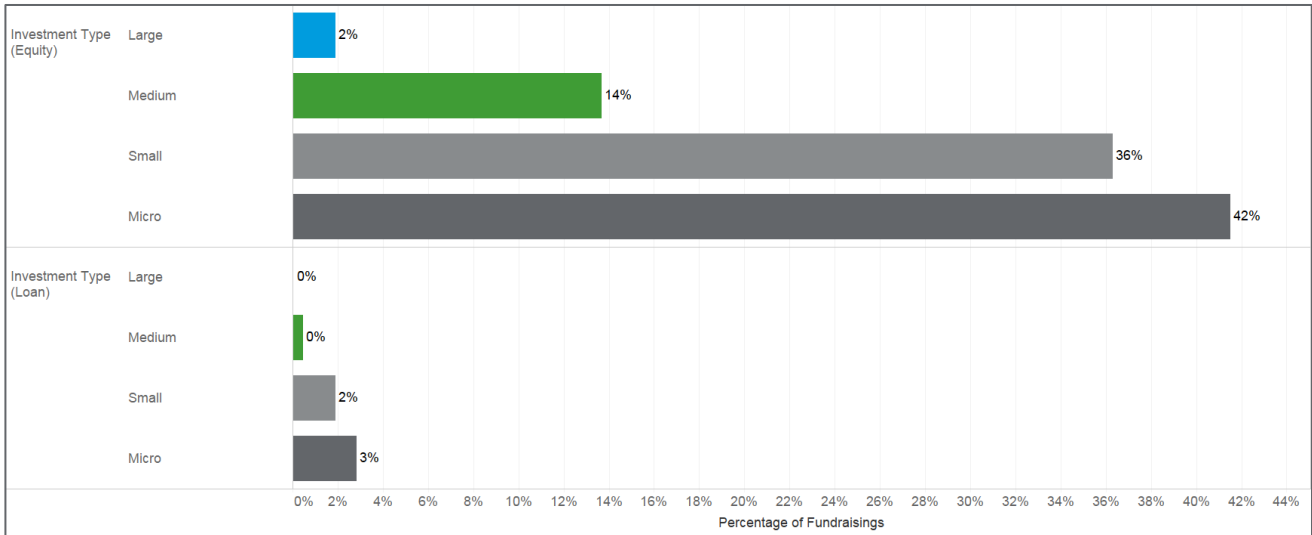


Source: Beauhurst (September 2017)

2.7.6 By Type of investment

Figure 26 sets out the percentage of deals whereby equity and or loan funding was the provider of funds. 95% of identified fundraising is through equity fundraising, whereby only 5% represents either loan funding (or a 'mix' of equity and loan funding)⁵⁹.

Figure 26 Type of Investment (Equity / Loan) by Percentage of Deals



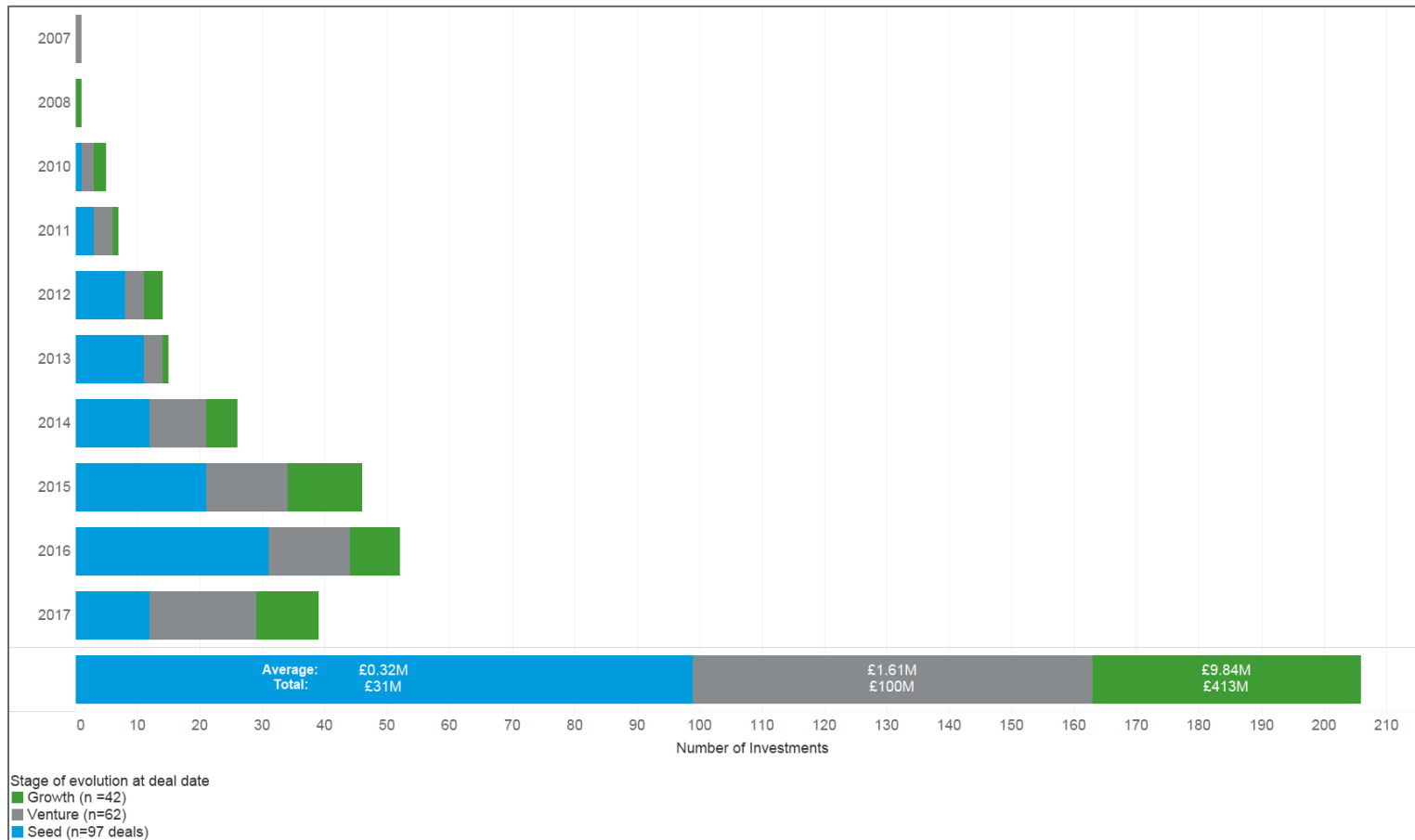
Source: Beauhurst (September 2017)

⁵⁹ Please note that loan funding may be underrepresented in this sample as Beauhurst is not fully comprehensive on loan coverage.

2.7.7 Number of investments by year, by stage of evolution

Figure 27 sets out the total number of investments, value (total and average) by stage of evolution at deal date. Definitions of seed, venture and growth investment funding can be found in Appendix F.

Figure 27 Number of investments by year, by stage of evolution



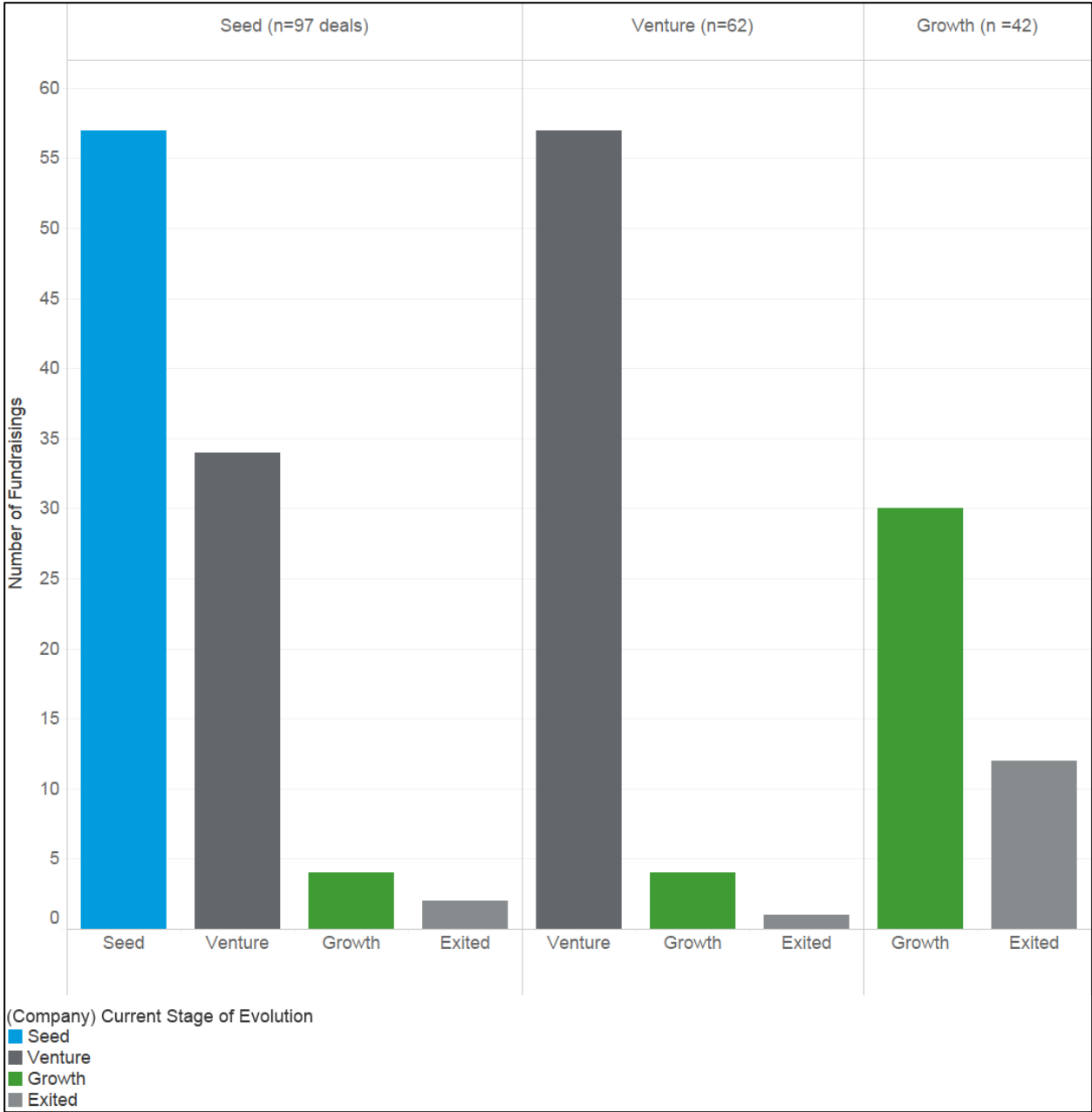
Source: Beauhurst (September 2017)

2.7.8 Company Evolution over Time (Time of Deal and Current Status)

Figure 28 sets out the company evolution over time (where a firm has identified its investment status at the deal, and afterwards). The y-axis sets out the number of known fundraisings, whilst the top of each column reports the number of firms.

This signals that approximately 20 of the 54 firms with fundraising which were seed are now either venture or growth firms, demonstrating real potential for scale-up with investment within the sector. This is an encouraging message, and further analysis of firm based transition from seed funding to growth should be undertaken. Further, four firms have moved from venture to growth. Only seven firms have exited (however, this means they have been purchased by another firm or group or merged).

Figure 28 Company Evolution over Time (Time of Deal and Current Status)



Source: Beauhurst (September 2017)

2.7.9 Funders

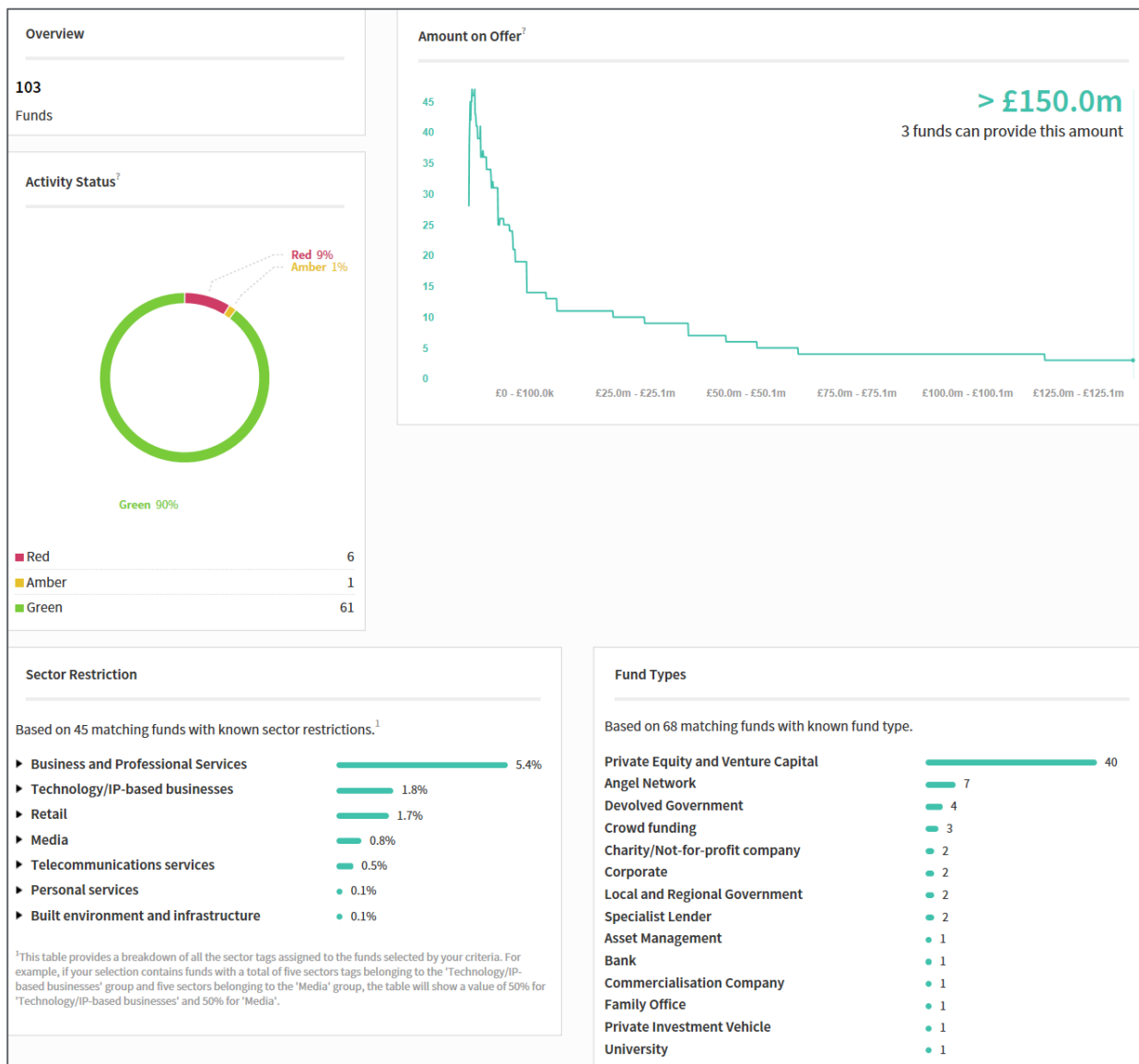
Figure 29 sets out an overview of the funds responsible for the investments identified. In total, there are 68 funds involved identified by Beauhurst, of which 90% are still in place. The remaining 10% are no longer operational or are unknown. Beauhurst analysis of the investments provides an overview of the number of funds which can provide investment to a threshold.

This identified only three funds which can provide over £150m for cyber security firms; however, as noted the largest investment identified in this dataset is Darktrace (c. £80m).

However, these findings are consistent with respondent feedback that the UK's venture capital landscape can perform for smaller scale investments (<£25m) but few funds are available, or indeed necessarily willing or able, to provide larger Series A investments to the sector.

This may warrant further granular research into the investments to date, the reason for investment, the funder, and performance to date.

Figure 29 Overview of Funds Available to these Investments



Source: Beauhurst (September 2017)

3. REGIONAL ANALYSIS

3.1 Introduction

This chapter sets out the analysis undertaken by RSM for the Department for Digital, Culture, Media and Sport (DCMS) in identifying cyber security businesses that could be considered part of identifiable clusters.

This sectoral analysis has included regional analysis of the UK sector based on the 'Registered Addresses' of UK firms. However, this has a clear weakness in that it may fail to identify UK firms with activity in multiple regions across the UK, as well as firms which may register in one location, yet not typically trade from the registered location.

For the purposes of a high-level regional analysis, it is important to provide a regional estimate of cyber security activity in the UK, based upon wider understanding of current regional clusters. These are particularly well understood where networks have been well established in recent years to support the development of the sector e.g. within the devolved regions, Cheltenham and Malvern. RSM consulted with several policy and sectoral stakeholders across different regions of the UK and carried out desk research in order to understand in more detail the activity of cyber security firms in those regions.

Based on the consultations and desk research, the table below sets out a 'high-level revised estimate' for the activity of UK firms in each region. Please note, the analysis recognises the risk of a) double-counting and b) false attribution of activity to regions (where full information may not be available for either number of firms, employment or revenue at the regional level i.e. some firms consulted do not break-down their figures in such a way), and c) recognises that regional analysis conducted to date will utilise a different definition or taxonomy to this study, and therefore firms included in regional analysis may not fully match this study and vice versa.

Table 12 outlines the percentage of total UK activity in cyber security for each region, firstly based on the RSM estimate and identified registered location (based on number of firms). The second column sets out a revised estimate based on consultations and further research.

Table 12 Activity by region (%)

Region	RSM 'bottom-up' estimate	Revised RSM Estimate
Greater London	31.6%	29%
South East	23.1%	21%
South West	10.1%	10%
East of England	7.2%	7%
Yorkshire and the Humber	3.4%	3%
East Midlands	3.1%	3%
West Midlands	6.4%	6%
North East	0.8%	1%
North West	4.6%	5%
Scotland	2.8%	7% ⁶⁰
Wales	4%	4% ⁶¹

⁶⁰ Scotland has been informed through consultation identifying approx. 70 firms in the region active within the space; however, examination of the known reporting in the region suggests that many of these firms may not be clear providers of cyber security products and services (yet may have employment in related areas to support the financial sector for example). For this region, RSM estimate 7% of the UK activity in Scotland as a high-level estimate.

⁶¹ Within Wales, there are well-regarded North and South Wales clusters, as well as a small number of well-established firms e.g. Airbus, Alert Logic, Rapid7 (See https://tradeandinvest.wales/sites/default/files/cyber_security.pdf) with a combined employment in Wales of c. 1,100 persons. However, the clusters also indicate a wide range of SMEs and micro-

Northern Ireland

| 2.8%

| 4%⁶²

These revised estimates reinforce that using the registered address of firms will under report the number of firms in the regions outside of London and the South East. Whilst this report welcomes engagement with representatives and champions of the sector in Scotland, Wales and Northern Ireland, there may be further analysis required for some of the English regions. However, overall RSM estimate that approximately 84% of revenue and/or employment is likely to exist within England, and 16% in the devolved regions.

Further research may therefore be merited to:

- Further investigate the number of firms in English regions as our revised estimates focused mainly on revising estimates for Wales, Northern Ireland and Scotland based upon devolved understanding of the sector;
- Exploring each of the firms further at the regional level (on a smaller scale) and building up to inform a granular analysis of revenue, employment and GVA by taxonomy category;
- Undertaking further analysis of linkage between known clusters and/or networks, and evaluating the relationship between known public investments in cyber security infrastructure and support and subsequent business activity and growth (as part of the sector's 'Develop' strategy strand).

firms, and for this reason, an estimate of 4% of the UK sector is considered reasonable.

⁶² Within Northern Ireland, CSIT and InvestNI have conducted estimates of the sector (c. 1,200 FTEs across approx. 35). For this reason, an estimate of 4% of the UK sector is considered reasonable.

3.2 Defining Economic Clusters

The concept of economic clusters with associated competitive advantage and positive externalities is often linked with the work of Michael Porter (1998)⁶³. Clusters effectively refer to the concentrated density of firms within a geographic region, albeit are not always limited to geographic co-location (they can include participation in networks, and supply chains).

There are economic benefits that arise from cluster participation at the firm level including enhanced access to skills (clusters tend to be urban as larger population sets drive larger regional economies), reduced costs (supply chain integration and ease of market access), and knowledge spill-overs (as evidenced through several UK wide cyber security networks with membership models and events within and external to the cyber security sector).

BEIS defines a 'competitive economic cluster' as a 'concentration of related industries and services in a location, including companies, their suppliers and clients; providers of knowledge services such as education, information, research, and technical support; and government agencies' (2017)⁶⁴.

In identifying economic clusters, whilst a high geographic concentration of firms is often the factor to address, this can also consist of identifying areas with strong firm growth from a more limited base, or through relative economic prosperity in the region (e.g. higher earnings relative to other sectors).

A further distinction to be made is between 'clusters' and 'networks'. Whereas a cluster is an amalgamation of interconnected institutions providing similar goods or services and supported by a wider range of institutions located nearby (all of whom drive for innovation), a network is an alliance of firms that work together towards an economic goal working either horizontally (within the same market) or vertically (between markets)⁶⁵.

3.2.1 Background:

With regard to the cyber security sector within the UK, there is clear benefit in identifying clusters as this enables enhanced understanding of where, how and why firms are setting up and selling cyber security products and services, and how this interacts with wider investment and activity within government and academia.

Clusters are therefore essential for economic analysis⁶⁶;

- Clusters contribute to economic growth: 31 clusters identified by McKinsey⁶⁷ were found to contribute to 20% of UK output whilst only containing 8% of UK businesses. The UK's top 10 clusters contribute (approx.) £200bn in GVA to the UK per annum.
- Clusters bring business advantages such as networks and connections which not only promote a better understanding of demand, but also support innovation.

However, clusters face obstacles such as increased demand for limited skills, access to finance, management regulation and availability of infrastructure. In identifying regional barriers, governments and private organisations can work together to reduce barriers to growth through increased funding and clear regulation.

⁶³ Porter, M (1998) 'Clusters and the New Economics of Competition'.

⁶⁴ BEIS, *Identifying Industrial Clusters in the UK*. 2017. Available at:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/661900/identifying-industrial-clusters-in-UK-methodology-report.pdf

⁶⁵ United National Industrial Development Organisation, *Clusters and networks development*. <https://www.unido.org/our-focus/advancing-economic-competitiveness/supporting-small-and-medium-industry-clusters/clusters-and-networks-development>

⁶⁶ McKinsey & Company, *Industrial revolutions: capturing the growth potential*. (2014). Available at:

http://www.centreforcities.org/wp-content/uploads/2014/07/FINAL_Centre-for-cities-report2014.pdf

⁶⁷ [ibid.](#)

Regional clusters drive innovation between businesses, academic centres and entrepreneurs which not only increases the rate of regional development, but also the collaboration between SMEs and large businesses to overcome challenges, as well as allowing SMEs to benefit from economies of scale. With cyber security, this is invaluable as it allows firms of all sizes to collaborate at a larger scale to ensure cyber security is not compromised. However, another benefit of having regional clusters is the ability to collaborate at an international level. One project which facilitates the international collaboration of clusters is Interreg Europe which helps to connect nine regions across Europe, all of which work together to ensure cluster policies are implemented efficiently. This is essential in ensuring that the clusters are working correctly and that SMEs can be inserted into global value chains and to facilitate the successful implementation of ris3⁶⁸. Strong regional clusters are also helpful in attracting foreign direct investment, as well as increasing productivity through specialised inputs and access to information.

3.2.2 Approaches to Identify Clusters

As set out in BEIS analysis, there are two traditional approaches in identifying clusters:

- **Case Studies:** Provision of detailed information on the relationships and entities within a sector / geographic area (usually in qualitative form)
- **Location Quotient:** Often used by Local Enterprise Partnerships (LEPs) (e.g. in Science & Innovation Audits). This identifies where there are greater than average (1.0) concentrations of sectoral employment within local areas. For example, a LQ of 5 would suggest that a region's employment is five times higher than would be expected at national level.

However, these approaches can be limited in that clusters are likely to form across administrative boundaries, and can be largely qualitative. Further, Location Quotients often rely upon Standard Industrial Classification (SIC) codes, and therefore may not capture regional variance in employment within hard to define sectors such as cyber security.

BEIS also set out the technique of Density-Based Spatial Clustering of Applications with Noise (DBSCAN) for the statistical identification of clusters from the bottom-up using co-ordinates of firms. Whilst this analysis does not seek to replicate that approach in full, density based modelling with ArcGIS of the known cyber security firms provides the following clusters. These are considered in line with the selected clusters within this analysis, but also provide insight that local knowledge is required to overlay known businesses prior to inclusion or exclusions of areas within cluster analysis. For example, the map below does not have GCHQ as a data point, yet this is well regarded as a core point in the development of the Cheltenham / West Midlands cluster. However, this analysis does support the selection of eight cluster areas for research purposes.

3.2.3 Heat Map Analysis of UK Cyber Security Firms:

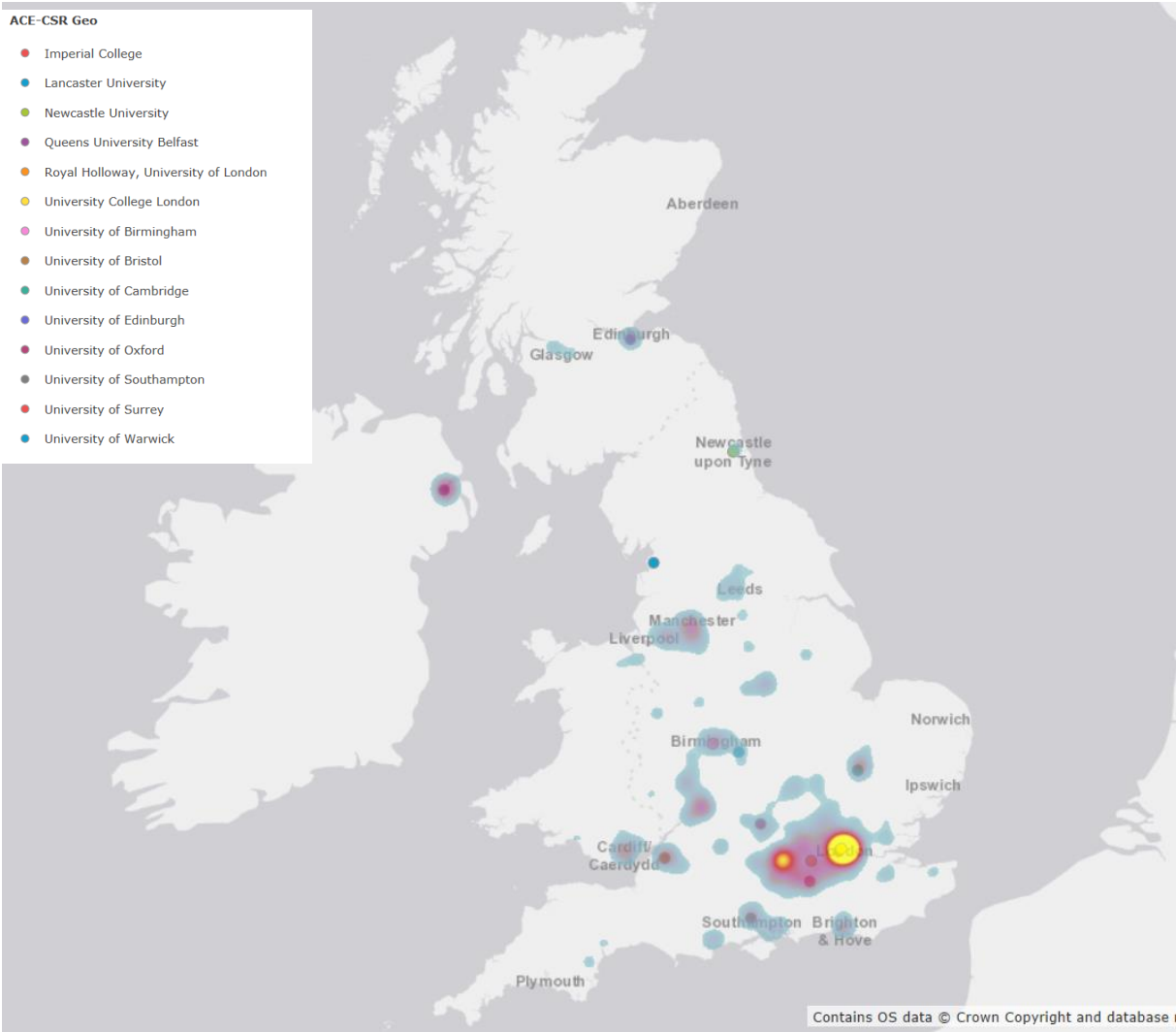
An initial heat map analysis of UK Cyber Security firms highlights concentration of firms within urban areas (with the highlighted regions spanning a population of over 32m people) in major cities such as London, Manchester, Cardiff, Belfast, Southampton, Birmingham, Leeds, Glasgow and Edinburgh.

Further, when overlaid with the Academic Centres of Excellence in Cyber Security Research (ACE-CSRs), there is a clear alignment between emerging cyber security clusters and the presence of ACE-CSRs, with only University of Warwick not within a 'cluster' area. However, this does not evidence the determinants of this relationship (where universities follow industry, or vice versa, or collaborative expansion). This will be explored in each of the clusters.

Figure 30: Heat Map of UK Cyber Security Firms and Relationship to Academic Centres of Excellence in

⁶⁸ <https://www.interregeurope.eu/>

Cyber Security Research



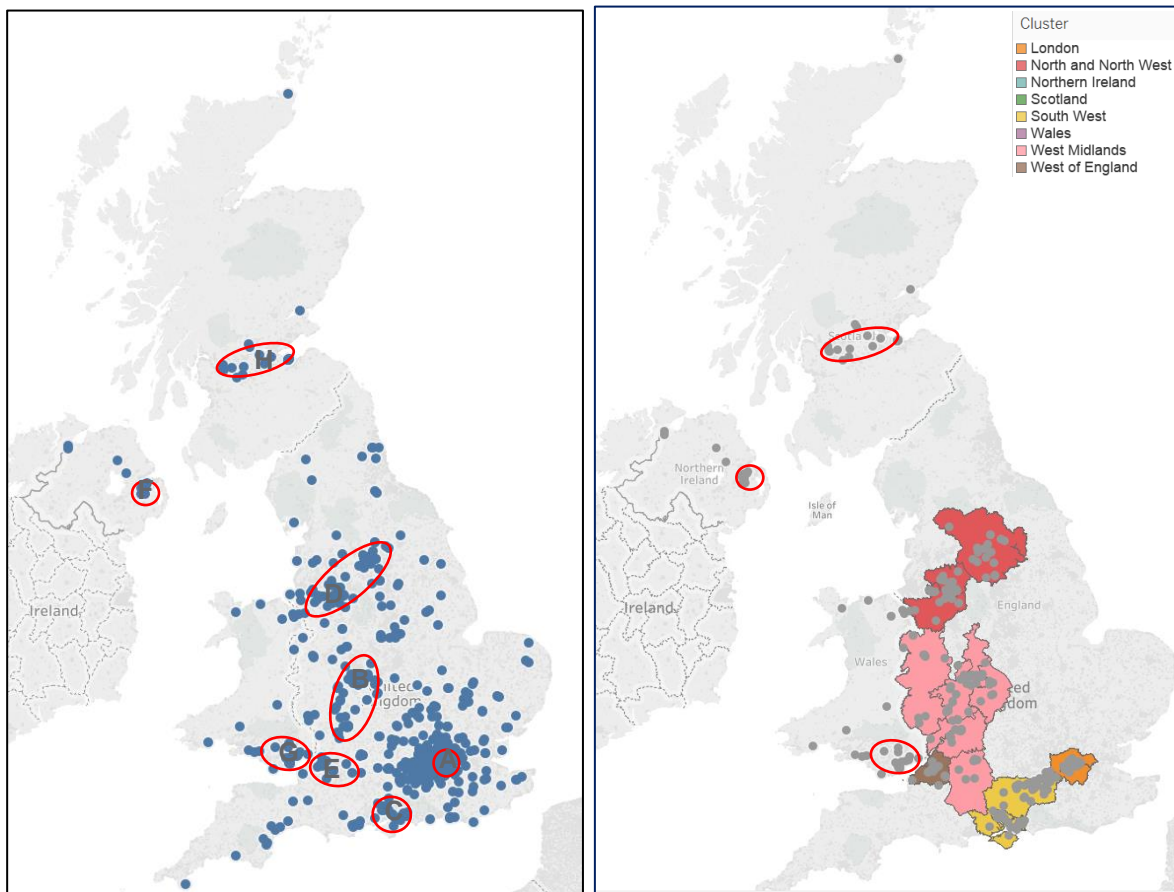
Source: RSM

3.3 Selecting Cyber Security Clusters

In 2014, the UK Cyber Security Strategy set out fourteen known emerging clusters⁶⁹ (at various stages of development) of economic activity. The UK Cyber Security Sectoral Analysis undertaken by RSM validates the higher concentration of cyber security firms in these cities and regions. However, there is known variance between the size and scale of these clusters (for example, London is home to more than 400 cyber security firms). Within the Cyber Security Sectoral Analysis undertaken in November 2017, 846 cyber security firms were identified across the UK, with the following geographic distribution. From initial review, there were several areas with cluster attributes (with visible density of firms within a selected radius). These are highlighted in Figure 10 below, and overleaf. These reflect a selection of clusters for research purposes. We recognise in the selection of these clusters that there are:

- Other 'clusters' of economic activity in cyber security (particularly in the immediate area external to Central London in addition to Oxford, Cambridge, Newcastle, Nottingham);
- Local Units within the cyber security market may not be well covered by this analysis, as the location is determined by *registered postcode* analysis, and therefore may undervalue the extent of sectoral activity across the regions (particularly in devolved regions whereby firms may register in London e.g. due to FDI, yet undertake market activity from Belfast, Cardiff, Glasgow etc).

Fig 31: Map of UK Cyber Security Businesses (in line with taxonomy)



It is worth noting that these reflect enterprises at the registered level, and therefore local unit data would provide a more granular assessment of cluster activity.

⁶⁹ Bath; Cambridge; Exeter; London; Kent; Malvern; North East; Northern Ireland (Belfast); North West; Scottish (Edinburgh); South Wales (Cardiff); Sussex (Brighton); Solent (Southampton); Thames Valley (Reading).

Table 13: Number of registered active cyber security firms by cluster

Cluster	Geography	Number of Active Cyber Security Firms	Estimated Cyber Security Employment	Estimated Cyber Security Revenues	Estimated GVA
A) Central London ⁷⁰		227	8,661	£1.53bn	£669m
B) West Midlands	Black Country Greater Birmingham and Solihull Coventry and Warwickshire Worcestershire Swindon and Wiltshire Gloucestershire The Marches	67	936	£66m	£31m
C) South	Solent LEP Enterprise M3	81	7,863	£1.63bn	£680m
D) North/North West England	Leeds City Region Greater Manchester LEP Cheshire and Warrington LEP	53	1,944	£200m	£87m
E) West of England	West of England LEP	18	352	£29m	£13m
F) Northern Ireland	Region	25	336	£20m	£13m
G) Wales	Region	37	342	£323m	£28m
H) Scotland	Region	22	238	£30m	£9m
Total		530	20,672	£3.83bn	£1.53bn
		(63%)	(66%)	(68%)	(65%)
Other (Not in identified cluster)		316	10,667	£1.85bn	£820m
		(37%)	(34%)	(32%)	(35%)
All Firms		846	31,339	£5.68bn	£2.35bn

For DCMS or any other body wishing to engage with the defined clusters, RSM has identified the core LEPs which best encompass the core cyber security activity within each respective region in England, and explore the devolved regions separately.

LEPs have a local responsibility to engage with and promote the local economy, particularly businesses that contribute to the goals and employment within the LEP. As such, any future investment nationwide in cyber security should look upon the role of these LEPs in disseminating funding and other support mechanisms to grow the local ecosystem of cyber security companies located within the cluster.

⁷⁰ We recognise the intensity of economic activity across London, including Thames Valley; however, we focus on Central London for purposes of analysis into how clusters are established.

3.4 Limitations in Cluster Analysis at Registered Level

Within the identified clusters of activity, these are estimated to cover:

- **63% (530) of cyber security businesses in the UK;**
- **66% (20,672) of UK cyber security employment, and 68% (£3.83bn) of revenues (within the sector, excluding cyber insurance and internal functions)**

However, it should be emphasised that given the cyber security sectoral analysis was UK focused at the registered level, this is considered to have underestimated the economic activity actually undertaken in Scotland, Wales, Northern Ireland and the regions (as a number of firms active in the regions will register in London and the South East and subsequently expand operations whilst remaining ‘based’ in London and the South East. This skews the regional analysis.

Table 14 outlines the percentage of total UK activity in cyber security for each region, firstly based on the RSM estimate and identified registered location (based on number of firms). The second column sets out a revised estimate based on consultations and further research.

Table 14: Activity by region (%)

Region	RSM ‘bottom-up’ estimate	Revised RSM Estimate
Greater London	31.6%	29%
South East	23.1%	21%
South West	10.1%	10%
East of England	7.2%	7%
Yorkshire and the Humber	3.4%	3%
East Midlands	3.1%	3%
West Midlands	6.4%	6%
North East	0.8%	1%
North West	4.6%	5%
Scotland	2.8%	7% ⁷¹
Wales	4%	4% ⁷²
Northern Ireland	2.8%	4% ⁷³
UK	100%	100%

⁷¹ Scotland has been informed through consultation identifying approx. 70 firms in the region active within the space; however, examination of the known reporting in the region suggests that many of these firms may not be clear providers of cyber security products and services (yet may have employment in related areas to support the financial sector for example). For this region, RSM estimate 7% of the UK activity in Scotland as a high-level estimate.

⁷² Within Wales, there are well-regarded North and South Wales clusters, as well as a small number of well-established firms e.g. Airbus, Alert Logic, Rapid7 (https://tradeandinvest.wales/sites/default/files/cyber_security.pdf) with a combined employment in Wales of c. 1,100 persons. However, the clusters also indicate a wide range of SMEs and micro-firms, and for this reason, an estimate of 4% of the UK sector is considered reasonable.

⁷³ Within Northern Ireland, CSIT and InvestNI have conducted estimates of the sector (c. 1,200 FTEs across approx. 35). For this reason, an estimate of 4% of the UK sector is considered reasonable.

3.5 Implications / Research Approach for Cluster Analysis

The UK Cyber Security Sectoral Analysis identified companies across the UK involved in the delivery of cyber security products and services, and this has informed (primarily, but not fully) the identification of eight clusters for research purposes.

In recognition that **registered companies** will not provide the granularity that **local unit** data would provide for cluster analysis, the research undertaken in the remainder of this chapter sets out high level economic estimates, overview of company activity (registrations, activities, employment etc), in addition to setting out how these interact and have been shaped by investments in wider public infrastructure, networks, and market development for cyber security.

Therefore, the clusters are selected for analysis to understand how they have developed in recent years, and to understand the underpinning rationale (where possible) for this growth, recognising there will be a **wide range of determinants for business activity**.

These can include:

- **Access to existing markets and complementary business:** Working collaboratively with organisations within a close physical proximity provides ‘value added services close to the end user’. For instance, a financial institution with a cyber security firm located close by may be able to work collaboratively with the security firm to offer the client, increased security and an overall competitive advantage for the financial institution. Porter comments that with increasing globalisation and the ability to access information more readily, competitive advantage ‘lies in local things – knowledge, relationships and motivation – that distant rivals cannot match’.
- **Access to Organisational and Technological Innovation:** Competitive advantage is derived through innovation and clustering is a driver for this. Geographical concentration is a key driver for organisational and technological innovation.
- **Research Institutions:** the rationale for the proximity of clusters to research institutions and universities is twofold and significant. Firstly, the universities produce a high number of skilled graduates, which cyber security organisations can employ thereby saving costs of recruitment and ensuring a high flow skilled labour is always present. Furthermore, many cyber security organisations run internship programmes with many universities’ technology departments which helps to strengthen the relationship with the institutions as well as to provide ‘preliminary’ training to graduates at a lower cost. This is a benefit that Marshall has also identified, surrounding clusters. Secondly, research conducted by universities regarding cyber security, ensures that cyber security organisations with strong collaborative links are at the forefront of any developments and are able to improve the value-added delivered to the end client. **From a demand perspective, clients can reduce their search costs and are able to locate businesses with a strong reputation, within the cluster.**
- **Relevance:** Mazur et.al.⁷⁴ identify three types of clusters; innovation, industrial and regional. With regards to cyber security, the clusters are ‘innovation clusters’, which are ‘information unions of various organisations allowing the use the advantages of the in-house structure and market mechanism that has the potential to distribute knowledge and information more quickly and efficiently. The success of these clusters is contingent upon the up-to-date sources of knowledge and state-of-the-art technologies, further explaining why cyber organisations choose to locate close to universities and research organisations.

⁷⁴ Mazur, V.V., Barmuta, K.A., Demin, S.S., Tikhomirov, E.A. and Bykovskiy, M.A., 2016. Innovation clusters: Advantages and disadvantages. *International Journal of Economics and Financial Issues*, 6(1S).

- **Access to Public Driven Market Development:**

- **Existing industry demand;** within each region, a prevalent industry (finance, healthcare, government, defence) is requiring cyber security services, thereby signalling available demand. Cyber security organisations will inevitably aim to satisfy that demand through locating nearby and forming clusters and regional specialisations.
- **Supporting institutions;** each region has access to a base of skilled employees from nearby universities, as well as collaborative opportunities with research and academic institutions. This allows cyber security organisations to employ top tier talent and ensure their products and services are 'cutting edge'.
- **Funding;** funding from private organisations and government agencies acts as a further signal for cyber security demand and acts as a driver for further clustering in the regions (with enhanced funding increasing the size of the market, encouraging new entrants and reducing drop-offs due to capital shortage).
- **Existing Networks:** A number of businesses may simply cluster in a region due to pre-existing market development. For example, where a region has an intensive concentration of activity in an aligned area e.g. a number of large IT software development firms, there can often be a growth in new market entrants where existing staff set up their own firms and join and grow cyber security start-ups.

4. EXAMPLES OF CLUSTERS

4.1 Cyber Security Clusters

4.1.1 USA Cyber Security Clusters

The US cyber security market consists of almost 40% of the global cyber security revenues.

Due to the significant size of the marketplace, the US cyber security sector is segmented by industry so clusters are therefore clearly identifiable and located throughout the country. An international assessment of clusters conducted by the Australian Government⁷⁵ found that the incumbent, established clusters existed within the US included;

- The San Francisco Bay Area;
- DMV (Washington D.C., Maryland and Virginia);
- Massachusetts (Boston);
- New York Tri-State Area; and
- The San Antonio-Austin Corridor

Clusters are also emerging throughout the country in cities such as Atlanta, Chicago and Houston.

The bulk of the report focussed on the existing clusters and what was noticeable, was that cyber security clusters formed around the predominant industry in the region. For instance, the San Francisco Bay Area is home to the most software security firms in the United States⁷⁶ and produces skilled cyber security graduates from Stanford University and Berkeley. The region also benefits from the highest level of investment of any region in the US⁷⁷ (\$12 bn) and technology powerhouses such as Apple and Google also are headquartered in the region. Overall the Bay Area region provides a strong base of employees as well as firms with whom to collaborate with and 'cluster' around.

Following the San Francisco pattern, the DMV region is home to government agencies and as such, the cluster in this region surrounds policy and government with the NSA research centre, CIA headquarters, National Cyber Security and Communications Integration Centre (NCCIC) and National Cyber Security Centre of Excellence, being located within this region. The requirement for cutting edge, cyber security solutions in this region is paramount in informing policy and collaborating with government organisations for military and intelligence gathering purposes. The Department of Energy also drives cyber security within the region and received \$20 million grant to develop cyber security tools for energy related infrastructure. Large private security organisations providing cyber security products and services such as Lockheed Martin, General Dynamics and Northrop Grumman are headquartered within the region to assist the government agencies.

In terms of healthcare, Massachusetts (Boston) is a leader in medical research and healthcare, home to world class institutions such as Harvard Medical School, Massachusetts General and Brigham and Women's hospital. The healthcare sector in the USA is increasing its spending more than any other sector relating to cyber security which may be attributed to cyber security attacks targeting the US healthcare sector in 2015, coupled with the strong government policy calling for protection of private data. The Advanced Cyber Security Centre facilitates collaboration between industry university and government organisations to allow increased knowledge sharing and provide cyber security solutions innovatively and effectively. Due to the increased call for cyber security in the region, large organisations such as IBM Security, Mimecast, RSA and Carbon Black act as sources of innovation and work collaboratively with the university organisations (Harvard and M.I.T.) to provide cyber security solutions.

⁷⁵ AusTrade (2016). *Cyber Security US Clusters Report - Austrade*. Australian Government.

⁷⁶ IBISWorld, *Industry Report 51121f: Security Software Publishing in the U.S.* (2016).

⁷⁷ PwC, *Investment by Region 2016*. (2016). Available at: <https://www.pwcmoneytree.com/CurrentQuarter/ByRegion>

The New York Tri State area is home to the US banking and finance industry which, like London, demands a high level of cyber security coverage, suffering the 3rd highest number of cyber-attacks of any industry in the US⁷⁸. Accordingly, JP Morgan and Citigroup spent a combined \$800 million on cyber security in 2016⁷⁹. The region is home to Columbia University, Princeton and Rutgers University Centre for Information Assurance. LexisNexis, IBM, DataMotion and Verizon are the large cyber security firms in the New York Tri State area.

The San Antonio-Austin Corridor (SAAC) is a defence focussed region, home to NSA facilities and DoD partnerships with private sector companies. Texas is home to the second highest percentage of software security publishing firms in the US and Austin alone boasts 46 incubators and accelerators. Collaboration amongst incubators, University of Texas, government defence organisations and private defence firms drives the innovation in the SAAC region, as evidenced by a 209% growth rate in cyber security roles between 2010 and 2014⁸⁰.

Analysis of the US cyber security sectors show that the reasons for cyber security clustering has three key reasons;

- **Existing industry demand:** within each region, a prevalent industry (finance, healthcare, government, defence) is requiring cyber security services, thereby signalling available demand. Cyber security organisations will inevitably aim to satisfy that demand through locating nearby and forming clusters and regional specialisations.
- **Supporting institutions:** each region has access to a base of skilled employees from nearby universities, as well as collaborative opportunities with research and academic institutions. This allows cyber security organisations to employ top tier talent and ensure their products and services are 'cutting edge'.
- **Funding:** funding from private organisations and government agencies acts as a further signal for cyber security demand and acts as a driver for further clustering in the regions.

4.1.2 Israeli Cyber Security Clusters

Cyber security in Israel is attracting a high level of investment and is helping to establish Israel as one of the world leaders in cyber security⁸¹. The evidence for this is established in the 2016 Israel Venture Capital Research Centre and ZAG law firm report which found that Israeli venture capital funds accounted for 16% of total cyber security venture capital funds, globally⁸² (second only to the US in terms of cyber security investment in 2017)⁸³.

The key area for investment is 'Silicon Wadi' (located in the major cities of Tel Aviv, Jerusalem and Haifa), consisting of 1500 start-ups and is home to organisations such as Google, Samsung, IBM, HP, Philips and Microsoft. The region also accounts for the most patent registrations per head in the western world, with IT accounting for 41% of these⁸⁴. However, reports find that investment is focussed more on supporting existing cyber security firms, rather than start-ups⁸⁵.

⁷⁸ IBM, *X-Force Cyber Security Intelligence Index*. (2016). Available at: <https://www.ibm.com/security/data-breach/threat-intelligence>

⁷⁹ Forbes (2015) Spending to Tackle Cyber Crime: Available at: <http://www.forbes.com/sites/stevenmorgan/2015/12/13/j-p-morgan-boa-citi-and-wellspring-1-5-billion-to-battle-cyber-crime/#cd96af61112b>

⁸⁰ Burning Glass Technologies (2015) Job Market Intelligence, *Cybersecurity Jobs*. Available at: http://burning-glass.com/wpcontent/uploads/Cybersecurity_Jobs_Report_2015.pdf

⁸¹ Forbes (2017) 'Six reasons that Israel became a cybersecurity powerhouse' Available at: <https://www.forbes.com/sites/gilpress/2017/07/18/6-reasons-israel-became-a-cybersecurity-powerhouse-leading-the-82-billion-industry/3/#21657073720e>

⁸² Reuters (2017) 'Israeli private high-tech firms raised \$5.2bn in 2017' Available at: <https://www.reuters.com/article/israel-tech-fundraising/israeli-private-high-tech-firms-raised-5-2-bln-in-2017-idUSL8N1PC26Z>

⁸³ Tech Crunch (2018) 'The state of Israel's cybersecurity market'. Available at: <https://techcrunch.com/2018/01/14/the-state-of-israels-cybersecurity-market/>

⁸⁴ Audi (2017) *Silicon Wadi*. Available at: <http://www.audi.com/en/innovation/futuredrive/silicon-wadi.html>

⁸⁵ See Source 83

Unlike the US, Israel's cyber security expertise is in traditional IT categories such as network security, mobile security and vulnerability & risk management. IoT also saw an increase in investment, particularly as exposure to connected devices grows globally⁸⁶.

The reasons why cyber security in Israel has proliferated over the last five years, particularly in Silicon Wadi include⁸⁷:

Government: The Government has identified cyber threats as a key risk that requires addressing and cyber security as an economic growth engine in which Israel could produce a competitive advantage. The goal is to place Israel 'among the top five countries leading in the field within a short number of years'. As such, the government ensures that start-ups and incumbent businesses within the sector are well supported.

Military incubators and accelerators: The government identified cyber security uses within the military sector, as such cyber security start-ups and individuals studying cyber security, are encouraged to derive applications within the defence and military sectors.

Investing in human capital: Israeli universities were amongst the first to offer cyber security specific courses and currently has six universities with research centres dedicated to cyber security. Cyber security is introduced into the curriculum at a high school ages and incentivised throughout education levels through the provision of grants and bursaries.

Embracing interdisciplinary and diversity: Cross subject integration, into cyber security is encouraged. For instance, at Tel-Aviv University, the Faculty of Arts was used to design a physical trojan horse virus, the purpose of which is to enhance the understanding of cyber security problems from different viewpoints.

Alternative approach: Israeli cyber security policy is comprehensive and focuses on longevity rather than addressing short term problems. The three-tiered approach ensures risks are mitigated sufficiently.

Although a significant member of the global cyber security market, unlike the US there is no regional industrial specialisation. Instead, there appears to be increased government involvement and greater integration of education within the cyber security objectives. A 'long term' approach is encouraged by the government and cyber security is seen as a proactive tool rather than a reactive one. It can be argued that the US sees cyber security as a reactive tool, investing in sectors only where there is demand rather than encouraging proactivity. Clustering as a result, is not wholly demand driven in Israel, but is facilitated by the government and its objectives.

⁸⁶ Ibid.

⁸⁷ See Source 82

5. UK CLUSTERS: KEY FINDINGS

5.1 Introduction

As set out in Section 3, there are a wide range of reasons for why cyber security firms will cluster in regions across the country. These can vary by the size, scale and offering of firms.

For smaller firms and start-ups, there may be a concerted effort to co-locate operations aligned to larger firms and universities to enhance product development and market credibility; but many of these firms may simply set up in a location that is of personal significance. This signals the importance of understanding further the granularity of business location (at the local unit level in addition to registered location).

For larger firms, many of these firms may be more diversified in nature (offer a wide range of other products and services), and therefore their location (at the registered level) is less likely to have been shaped by cluster development, but may have shaped their location decisions at local unit level, and also shaped investment decisions from smaller firms.

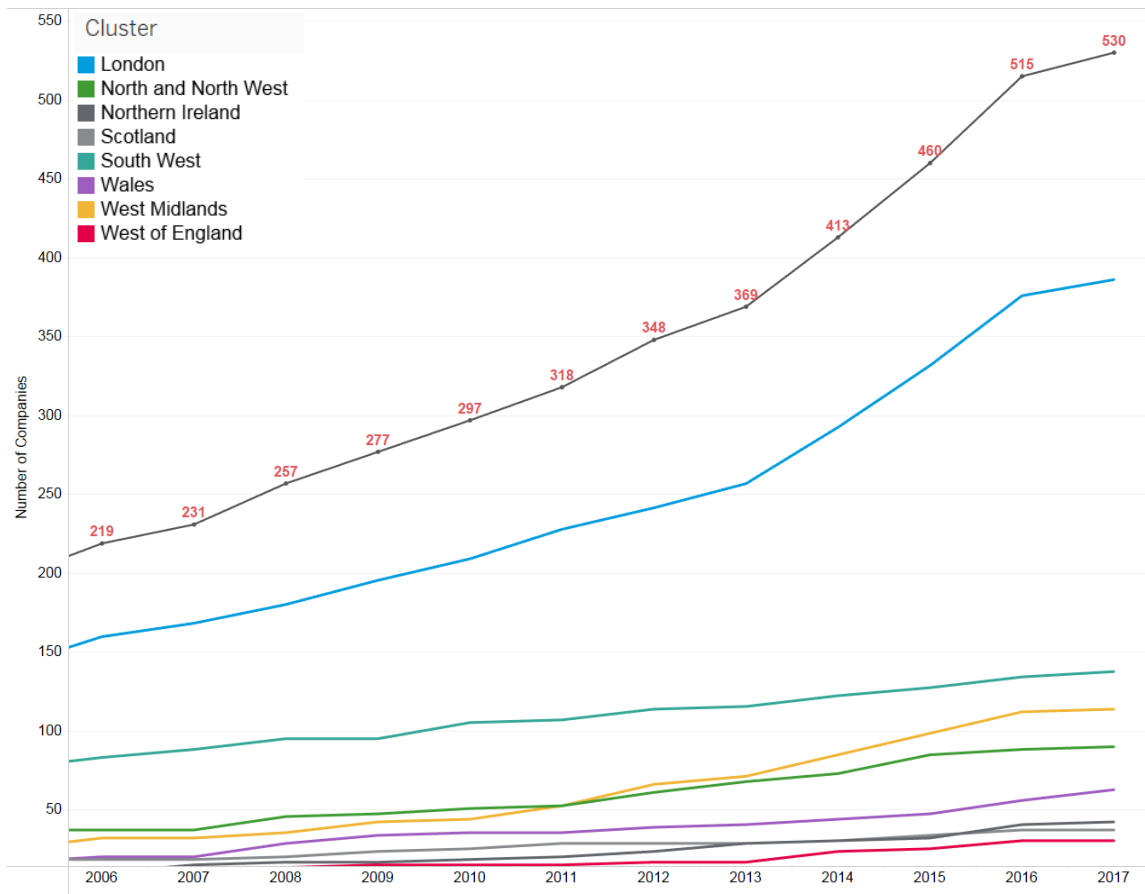
Analysis of regional business support and development assets has shown cyber security clusters can be driven by proximity of universities, large companies, funding and research organisations in addition to industry changes, for example: Southampton has a significant marine and maritime industry – the new BAE Systems base will develop driverless boats, whereby cyber security will play a key role.

The development of new technologies in existing markets will contribute to how cyber security firms locate (at the local level) e.g. Bristol may be shaped by its microelectronics and smart city initiative, and Belfast through its growth in professional services and knowledge economy. For regions such as London and Scotland, the finance sectors were predominantly the drivers for cyber security investment whereas drivers for clustering in the West of England was due to the presence of pre-existing, large technology, security and automotive firms.

A common theme across each of the clusters was availability and quality of cyber security talent. Most of the regions contained or were in close proximity to an Academic Centre of Excellence in Cyber Security Research, each of which have their own higher education cyber security degrees which will culminate in a well-supported cyber security labour force.

Across the clusters, there has been clear growth in the last five years within Central London (growing from over 150 firms in 2013 to more than 230 in 2017), and consistent growth across the regions. The West Midlands cluster has also demonstrated significant growth in company (see Fig 32) incorporations signalling new activity particularly around the Malvern and Cheltenham clusters.

Fig 32 Cluster Development (Number of Registered Firms by Cluster)

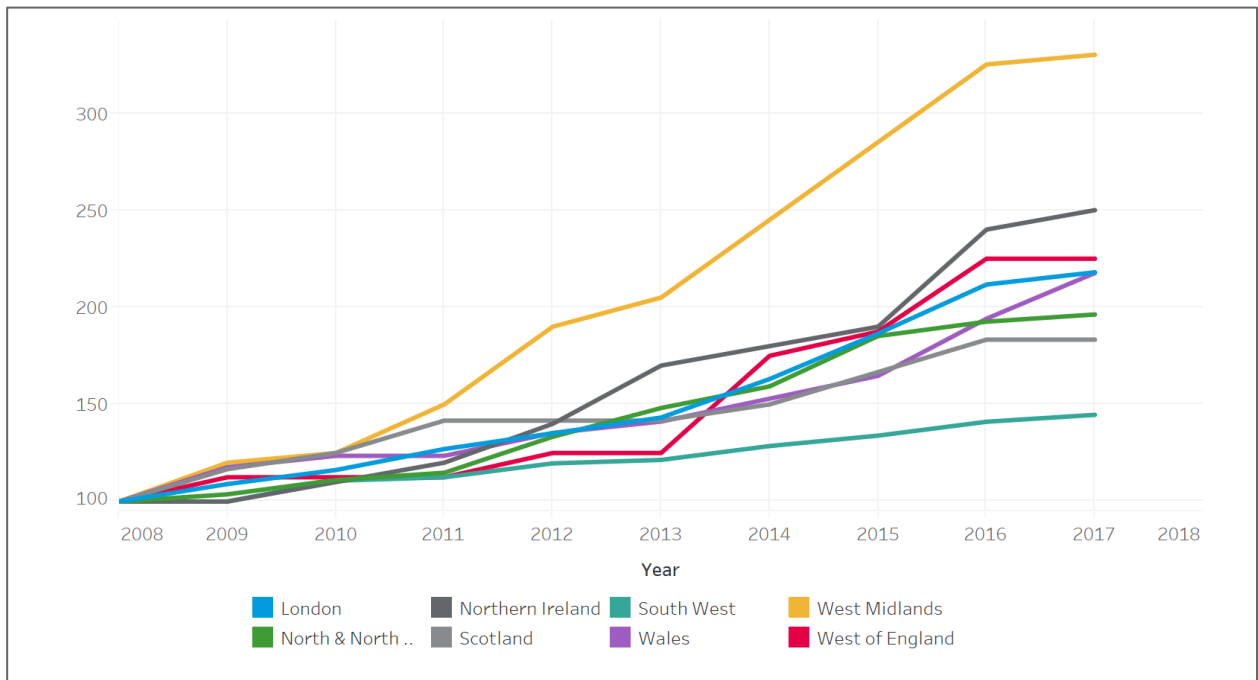


Source: RSM, Orbis

Figure 34 shows the growth in number of active cyber security firms by cluster, indexed with base at 2008=100. This allows us to observe the difference in growth rates among clusters in cyber security activity.

There is an obvious cluster leader, West Midlands, which has exceeded any other cluster's activity from 2011 onwards. There was a considerable uptick in new births of cyber security firms between 2013 and 2016 for this cluster, before tailing off in 2017. Within this period, 2015-2016 appears to be the most prominent year for activity across all clusters, with most witnessing a slowdown in growth thereafter.

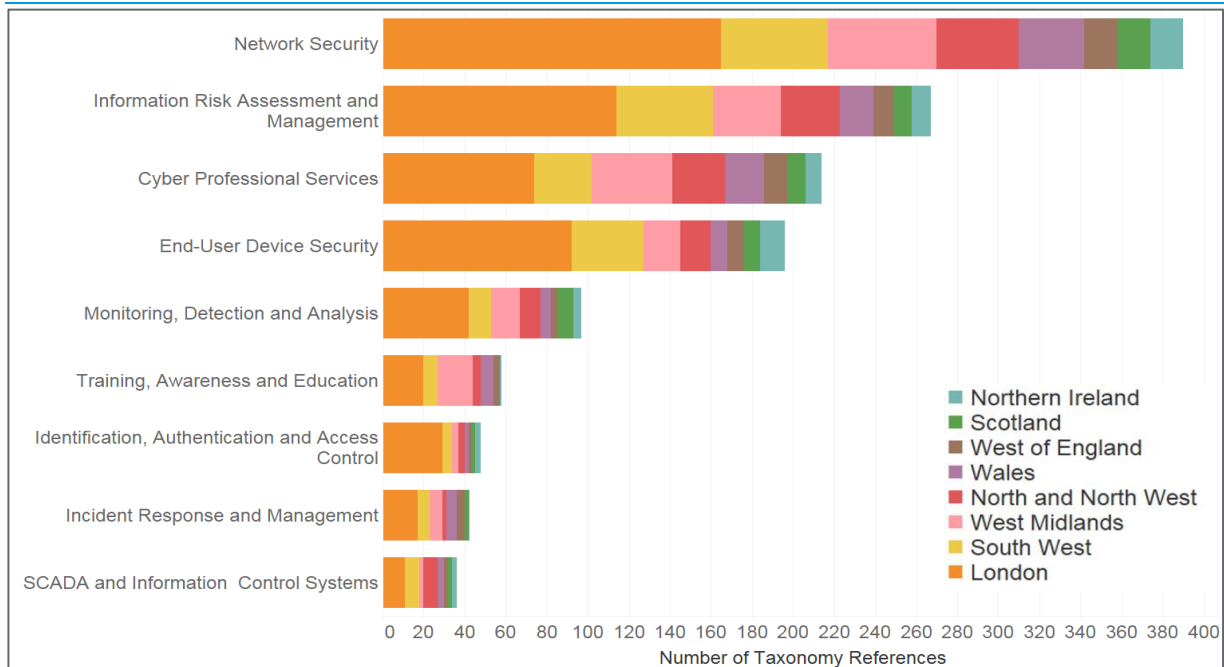
Figure 34: Growth in births of active cyber security firms across RSM clusters (2008 = 100 index)



Source: RSM, Orbis

Figure 35 also demonstrates that the clusters are relatively similar as the national picture with regard to service offering but do have some variance. For example, the West Midlands is proportionally strong with regard to network security, and London more limited in cyber professional services.

Fig 35 Taxonomy by Cluster



Source: RSM, Orbis

5.2 Selected Cluster Summary

Of the clusters researched, the table below sets out three of these with attributes worth further consideration and research to understand how these have developed and can be translated across the UK.

Cluster	Key Cluster Attributes
A) Central London	<ul style="list-style-type: none"> + Over 200 well-established cyber security product and service providers within Central London; + Clear alignment to public investment in cyber security, with government funding providing support to a growth industry (opportunities with proximity to a number of national cyber security institutions / new London Innovation Centre) + World-leading research capacity proximity (three ACE-CSRs in cluster) + Clear route to product and service provision for UK's hub for services e.g. financial services information risk assessment and management + Provision of high quality labour + Emerging growth appetite for VC investment - Potential limitations in office space, labour, and affordability without external investment - Taxonomy research indicates 'Cyber Professional Services' may not be as significant an activity (at the firm level) in Central London as other regions: this may indicate cyber security being undertaken at the firm level / through non-London providers for large firms based in London. This may create revenue / labour challenges for new entrants in the London market. -
B) West Midlands	<ul style="list-style-type: none"> + Clear backing for the cyber security industry from the relevant LEPs, including new Science and Innovation Audit, and investment in infrastructure. This has supported growth in number of firms. + Initiatives in place to support knowledge exchange and training despite lower concentration of ACE-CSRs e.g. University of Gloucestershire / Raytheon / GCHQ Degree Apprenticeship scheme aligned with wider government priorities for HE/FE + Market driven by innovation and changing market priorities by well-established manufacturing and defence sectors: significant opportunities for cyber security market embedding within emerging industries e.g. autonomous vehicles – Jaguar Land Rover + Clear messaging for investment / set-up in the region with cyber security and location of GCHQ, MoD, Dstl + Young population, with lower cost of business than in South – potentially compelling to FDI - May require support with skills development and VC investment (typically low)
Devolved Regions (Northern Ireland, Scotland and Wales)	<ul style="list-style-type: none"> + The devolved regions have been active in encouraging FDI in cyber security firms to the UK (e.g. Northern Ireland providing clear financial support to investors in recent years, and now a global hotspot for cyber FDI) – also clear investments for digital innovation. + Compelling for investment (lower costs for business base in cyber security, with young talented populations) + Each region has a small number of urban populations, which enables regional networks / communication to form - Risk of under-representation without use of local unit data / regional knowledge given company registration outside of the locations of activity



- Risk of small market saturation (NI and Wales – small population clusters, with low GVA, low productivity: this may cause challenges for cyber security firms in generating income. However, this can also provide opportunity for export driven growth)

6. CYBER SECURITY TAXONOMY

6.1 Introduction

For purposes of this study, RSM and DCMS utilised a cyber security taxonomy to support the definition of the cyber security sector, determine inclusion and exclusion criteria for firms, and to apportion the final list of firms by taxonomy component to understand in what area of activity firms are active.

This taxonomy is defined below. The analysis recognises the potential for overlap (where firms may conduct many components) or where a judgement call may be required to allocate an activity. All efforts have been made to minimise duplication and allow for the final list of firms to have been well-informed by the taxonomy as an input, as well as an output (firms by taxonomy).

Taxonomy Component	Guiding Definition
Information Risk Assessment and Management	This examines companies involved in providing products or services aligned to supporting organisations with IT risk assessment and management, with provision of support such as: Implementation of risk and security provision e.g. email filters; Threat, vulnerability and compliance management; and Security scanning and testing
Identification, Authentication and Access Control	Gaining access to computer networks is based on three key steps; identification, authentication and authorisation. Access may be granted through various login credentials including passwords, personal identification numbers (PINs), biometric scans, and physical or electronic keys. This component covers companies that supply goods or services that control access to computer software or hardware.
Network Security	Network security refers to any activity designed to protect the usability and integrity of a network and its data. It includes both hardware and software technologies. Effective network security manages access to the network. It targets a variety of threats and stops them from entering or spreading on the network.
End-User Device Security	In information technology, the term end user is used to distinguish the person for whom a hardware or software product is designed from the developers, installers, and servicers of the product. This component looks at firms that allow end users to access or interact with networks using secure devices. E.g. allowing employees to access their companies secure networks using portable devices.
Monitoring, Detection and Analysis	This component looks at firms that are involved in the monitoring or detection of varying forms of threats to a network or system. This could include firms that deal with network security monitoring, i.e. the collection, analysis, and escalation of indications and warnings to detect and respond to intrusions
Incident Response and Management	This component should include firms that deal directly with cyber threats or incidents. This could be either by offering products (hardware or software) to companies or by providing solutions to companies when incidents do occur, e.g. data loss, DOS attacks or various forms of hacking.

Taxonomy Component	Guiding Definition
SCADA and Information Control Systems	<p>Supervisory control and data acquisition (SCADA) systems monitor and control critical infrastructures of national importance such as power generation and distribution, water supply, transportation networks, and manufacturing facilities. The pervasiveness, miniaturisations and declining costs of Internet connectivity have transformed these systems from strictly isolated to highly interconnected networks. The connectivity provides immense benefits such as reliability, scalability and remote connectivity, but at the same time exposes an otherwise isolated and secure system, to global cyber security threats.</p> <p>An industrial control system (ICS) is integrated hardware and software designed to monitor and control the operation of machinery and associated devices in industrial environments. Therefore this category includes companies involved in the provision of these products and services.</p>
Training, Awareness and Education	<p>Firms that provide products and services in relation to cyber training, awareness or education.</p>
Cyber Professional Services	<p>Potential to use the definition used by the National Cyber Security Centre:</p> <p>Certified Cyber Consultancies will have demonstrated to NCSC that they have;</p> <ul style="list-style-type: none"> a proven track record of delivering defined cyber security consultancy services a level of cyber security expertise supported by professional requirements defined by NCSC the relevant Certified Professional (CCP) qualifications <p>Manage consultancy engagements in accordance with industry good practice</p> <p>Meet NCSC requirements for certified professional cyber services companies</p> <p>In wider terms this component should include firms that provide professional services or consultancy services (e.g. advice or implementation of solutions) that focus on cyber security.</p>

6.2 Taxonomy Key Terms

In line with these definitions, a list of c. 220 search terms across the taxonomy was drawn up in July 2017 to input into Orbis to identify any firms which might meet the criteria for including in the analysis (see Appendix B). Upon finalising the list of firms, a concise list was utilised to filter firms by taxonomy component. These include:

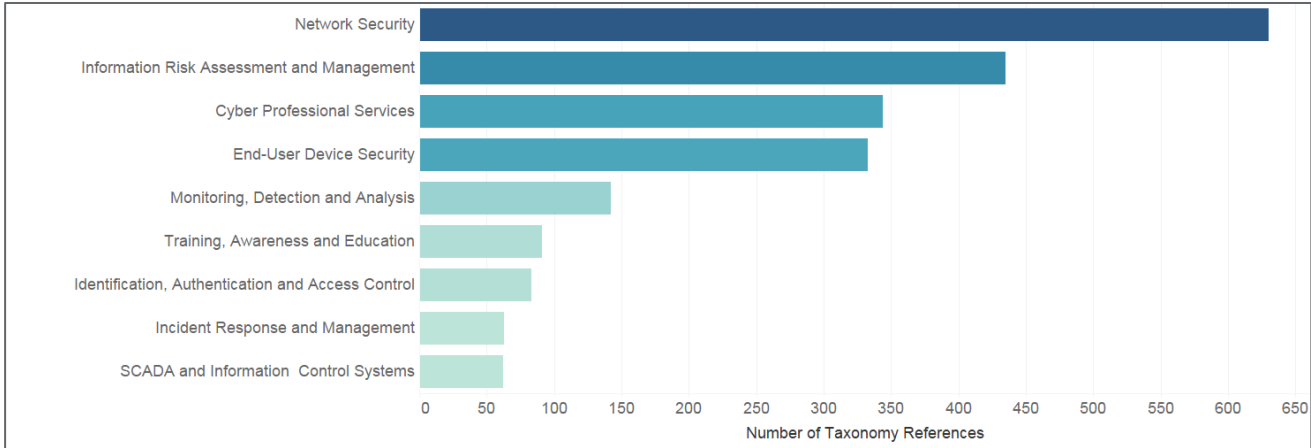
Taxonomy Component	Example Key Terms
Information Risk Assessment and Management	Risk Assessment/assess Governance Solution Assurance ISO27001 Vulnerability
Identification, Authentication and Access Control	Identity Authentication PKI User access Encryption
Network Security	Firewall Appliance Perimeter Network Security
End-User Device Security	Protection Root of trust Self-healing IoT / internet of Things Patch / Update Malware Antivirus
Monitoring, Detection and Analysis	Monitoring Detection Analytics Event Intrusion SOC Anomaly Intelligence Attack
Incident Response and Management	Incident Mitigation Forensics Security Information and Event Management (SIEM)
SCADA and Information Control Systems	Industrial control system /ICS SCADA

Taxonomy Component	Example Key Terms
Training, Awareness and Education	Awareness Training Certification (SANS; Crest; CISSP)
Cyber Professional Services	Penetration testing/Technical cyber security assessments Consulting Cyber security consultancy

6.3 Firms by Taxonomy

When the 846 firms identified to date as providing cyber security products and services were analysed against the taxonomy terms, this involved capturing the number of references each firm had against each part of the taxonomy within each firm’s trade description and or products and services. This yield 2,183 ‘hits’ i.e. each firm had approximately 2.6 words linked to the taxonomy within its description. This is set out below in Figure 36.

Figure 36 All References (n = 2,183)

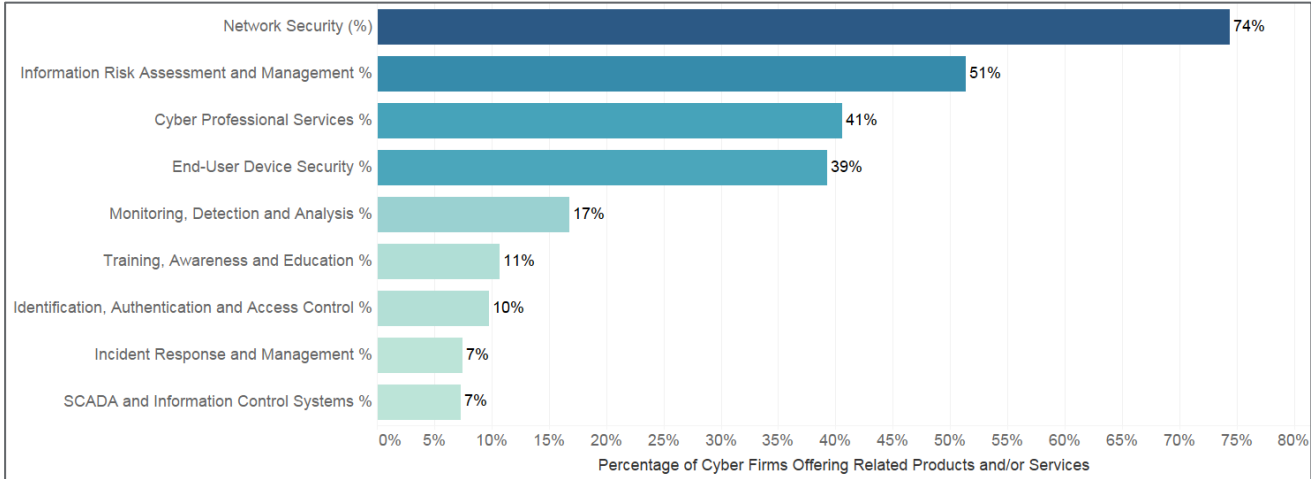


Source: Beauhurst (2017)

Figure 37 sets out the number of unique firms (n=846) which contain a reference to a particular taxonomy component. The majority of firms met the criteria for ‘network security (74%)’, followed by Information Risk Assessment (applicable to 51% of firms) followed by Cyber Professional Services (41%).

It is worth noting that in Figure 37, as the total percentages figures add up to approximately 250%, this would suggest that firms are active in several taxonomy areas e.g. strong overlap between ‘network security’ and ‘end-user device security’ product and service provision.

Figure 37 – Firms by Taxonomy (N=846)



Source: Beauhurst (2017)

7. SURVEY FINDINGS

7.1 Introduction

In addition to the collection of company data and telephone consultations with key stakeholders, RSM worked with DCMS to carry out an online survey of UK cyber security firms.

The purpose of the survey was to gather insights and views from the sector regarding the taxonomy outlined by DCMS, activity and employment within the cyber security sector, the regional dynamic of firm activities, estimation of remuneration and their views on skills and talent within the sector. A copy of the online survey and its questions is set out in Appendix E.

7.2 Responses

Overall, one hundred and seven (107) respondents completed the survey, with sixty-two (62) respondents providing full responses to each question. Participants ranged from small start-up cyber security firms to large scale multinational firms with cyber security divisions.

7.3 Key Findings

7.3.1 Revenue and employment

- Sixty-two (62) respondents to the survey provided full revenue and employment estimate responses. The total revenue of these firms was reported as £9.9 billion in the last financial year (2016/17).
- These firms estimated that approximately **£1 billion of revenues could be allocated specifically to cyber security activity.**
- For these firms, their total employment was estimated to be 40,066, with **5,155 of those employees specific to cyber security.**
- This provides a survey estimate of cyber security **revenue per employee of £194,000.** This compares to £181,378 using RSM company estimates, reflecting that the survey provides a useful insight and validation for this sectoral analysis.

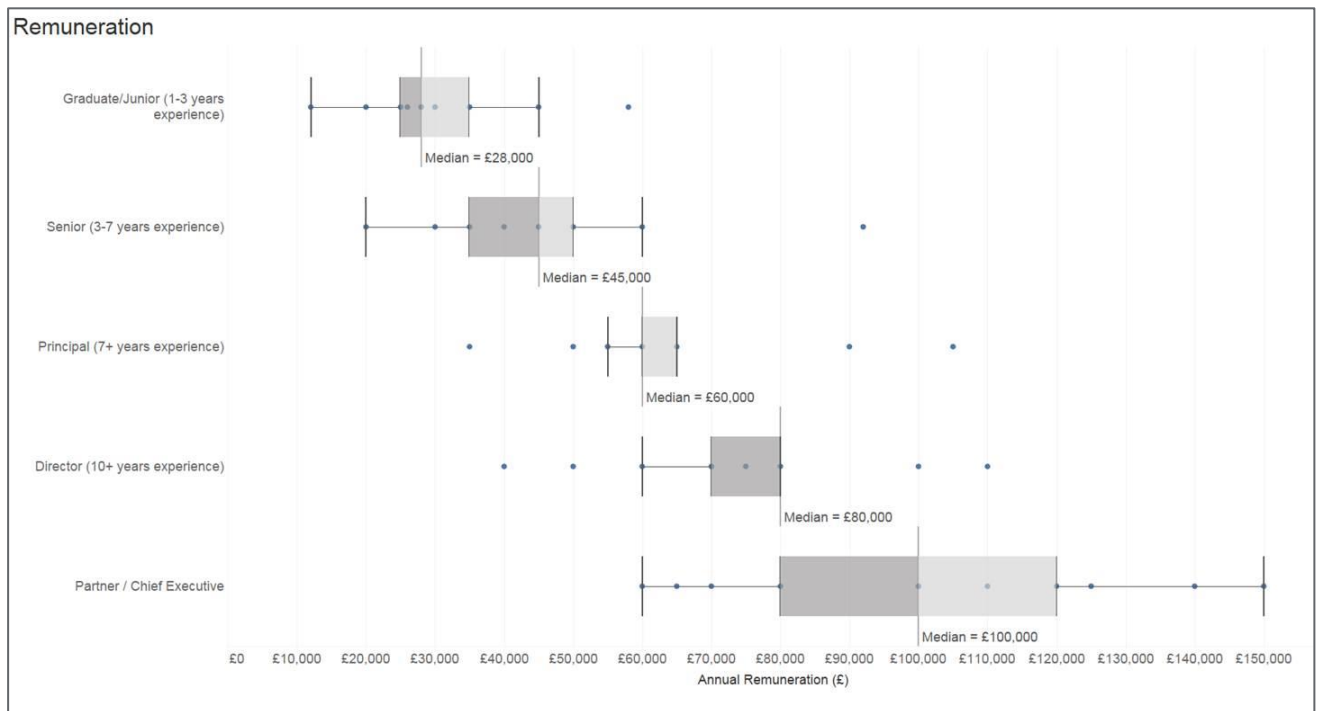
7.3.2 Cyber security in the regions

- Analysis of the survey responses suggested that the North West of England had the greatest percentage of cyber security employment with 29% of cyber security reported in the survey being attributed to that region. The South East and Greater London followed with 22% and 21% respectively.
- These estimates should be treated with caution due to the small sample size of our survey. However, this does provide further suggestion of significant employment clusters in cyber security in the South East and Greater London.

7.3.3 Employee remuneration

Figure 38: Annual Remuneration by Employee Level

- The chart above outlines the findings of the survey in relation to employee remuneration for employees with



a range of experience by each firm.

- Median remuneration values range from £28,000 for graduate/junior roles, £45,000 for senior roles, £60,000 for principal roles, £80,000 for director roles to £100,000 for partner/chief executive roles. This reiterates the wage premium within the sector.

7.3.4 Views on the taxonomy

- For the survey respondents, **the most reported area of the taxonomy that they provide cyber security products and/or services within was Cyber Professional Services with 58% of respondents** stating that they provide products and/or services in that area.
- The least reported area was **Supervisory control and data acquisition (SCADA) and Industrial Control Systems (ICS) with only 23% of respondents** stating that they provide products and/or services in that area.
- Typically, respondents suggested that they each provided products or services in **three areas of the taxonomy** suggesting that firms are offering a breadth of products and services in cyber security where operational e.g. penetration testing, risk assessment, threat detection, and consultancy support.

7.3.5 Skills in the cyber security sector

- The overwhelming view amongst respondents was that **there is a shortage of talent in the UK labour market when it comes to cyber security skills**. 90% of respondents suggested that the UK has some form of shortage of skills relating to the cyber security industry that impacted on their own firm.
- Respondents highlighted the lack of real world understanding or experience from graduates entering the labour market and the lack of tailored training programmes. They also noted **difficulties in filling job vacancies and high wages for people with the necessary skills**.

“This is the biggest challenge facing the sector. There is a worldwide competition for rare cyber security, data science, AI and engineering talent. The countries that best encourage and capture that talent will build the strongest cyber security industry.

Right now, the UK has access to 500m people across the EU and is an attractive destination. When we cut that to 60m post-Brexit the opportunity to build a big domestic industry will diminish. We can and should invest in training and education, but that takes time and start-ups have a tiny window to be successful [...]

If the Government does one thing to help UK cyber it would be to make it really easy for UK firms to hire top talent in the sector from other countries.”

CEO of UK Cyber Security Firm

“There is clearly an acute human skills shortage in the UK cyber security sector and combined with the relentless growth in criminal, industrial espionage, and nation state cyber-attacks the UK government should do more to facilitate and underpin cyber training, learning, and qualification in the UK.”

Director of UK arm of multi-national software firm

8. CONCLUSIONS AND INSIGHT

This sectoral analysis offers a bottom-up insight into the economic contribution of the UK's cyber security sector. For those 846 firms that have been identified as providing cyber security products and services, they are estimated to contribute:

- £5.7bn in revenue per annum;
- £2.3bn in Gross Value Added per annum;
- Employ an estimated 31,300 – 40,000 FTEs; and
- The number of firms has grown by over 50% in the last five years, and over 100 firms have been incorporated in the last two years. This shows that the market is developing and growing, and new entrants are commonplace to the UK Cyber Security sector.

For these reasons, it is crucial that DCMS and other organisations involved in supporting the delivery of the National Cyber Security Strategy can use this baseline analysis in the coming years to inform policy interventions. On this basis, RSM set out the following insights and resulting considerations as a result of this analysis below.

Baseline & Evaluation

As this sectoral analysis has been conducted from the 'bottom-up' i.e. identifying at the firm level and aggregating to inform the sectoral overview, this will enable DCMS to monitor the sector each year by identifying and exploring:

- New entrants to the sector:** for example, where a spin-out from an accelerator has resulted in a full business start-up which has operational revenue and employment;
- Firms exiting the sector:** for example, where a firm has ceased trading, or has been purchased by a competitor;
- Changes in firm sizes** e.g. where a firm has significantly increased its employment or revenue in a financial year;
- Identifying 'high-growth' firms or clusters** e.g. postcode areas in which firms are growing higher than the national average
- Track overall economic contribution of the sector annually** through headline revenue, GVA and employment figures;
- Evaluate business activity** in clusters supported by DCMS interventions or where cyber security assets are located e.g. effectiveness of Academic Centres of Excellence in Cyber Security Research in growing regional markets for cyber security.

Further Analysis of the Sector

There is also considerable potential for further analysis of the UK Cyber Security sector to be undertaken. We suggest that the next steps should include:

- Further investigation into regional activity of firms** (incl. regional statistics, or further Location Quotient (LQ) analysis, or analysis/evaluation of business activity in identified clusters);
- Further disaggregation of investment data** (e.g. exploring each investment into firms, by funder, for what purpose and associated outcome to explore the financing landscape for firms);
- Explore how best to monitor progress of SMEs** (particularly those firms identified that currently are not required to return their full accounts to Companies House) over the next 5 years to map out growth / changes in business structure and activity / investment progress and patterns; and
- Further engagement and research to understand **specific barriers and challenges for cyber security firms** based upon consultation findings e.g. access to labour, capital, and investment. This will enable the provision of evidence-informed interventions and supports to be provided to industry.

9. APPENDICES

9.1 Appendix A: Source List for Cyber Security Firms

The RSM Economic Consulting team gratefully acknowledge the input from DCMS in this assignment in supporting the identification and collation of a wide range (more than thirty) known cyber security networks, conferences, clusters and representative bodies across the UK and internationally. In addition, we are also appreciative of the feedback regarding regional cyber security activities obtained through consultation with representatives within devolved administrations in Scotland, Wales and Northern Ireland.

The following sets out the sources utilised to inform the initial long-list of cyber security firms operating within the UK. It is worth noting that over 4,000 firms and organisations were analysed for potential inclusion within this study's long list. For transparency, all firms were analysed within scoring criteria (Appendix C) aligned to the strength of sources, and trade description alignment to the cyber security taxonomy (Appendix B) used in this study.

Primary Data Sources:

- Bureau van Dijk (ORBIS platform);
- Tracker (RSM);
- Beauhurst

Orbis

Bureau van Dijk's Orbis platform is the primary source of company data used for this study. Orbis provides details on c.11m UK businesses based on Companies House records. The study has extracted information from the most recent financial accounts (2015/16) including but not limited to; revenue/turnover, profits, employee remuneration, depreciation and amortisation, employment numbers, registered company address and company descriptions.

It should be noted that as Orbis draws upon Companies House records, it contains less detailed financial information for smaller firms⁸⁸. This is because these firms are only required to provide abbreviated accounts to Companies House.

Tracker

The study uses RSM's in-house company information platform (Tracker) as a second source of company data, to validate company information, and to support with GVA estimates at a company level. Tracker also provides financial accounts from the previous three financial years (2013/14 to 2015/16), which have been used alongside the financial data collected in Orbis to provide an indication of changing patterns with regards to company financials.

Beauhurst

Beauhurst data is used to analyse private investment in UK cyber security firms (www.beauhurst.com). Beauhurst is a leading provider of investment data on high-growth and emerging firms in the UK, and tracks announced investments and grant funding. The firms identified within this sector study have been analysed against data held by Beauhurst regarding investments. This includes information regarding the level and the type of investments provided, the funding available to UK cyber security firms, and sets out the size and growth of the respective firms e.g. start-up, seed, venture, and growth. This analysis recognises that this captures investment only for identified firms as known by Beauhurst, and therefore it may not capture all investment in cyber security firms or activities.

⁸⁸ A company will be 'small' where it has any two of the following conditions: a) a turnover of £10.2m or less b) £5.1m or less on the balance sheet c) has fewer than 50 employees

Desk Review & Other Sources

As with any in-depth sector study, it has been necessary to draw upon desk research and additional sources to extract relevant and up-to-date information. The study has drawn upon LinkedIn to inform and validate estimated UK employment of cyber security professionals. In addition to this, it also provides information on the number of personnel within cyber security companies, and the locations of their sites, creating an additional layer of verification for these estimates.

Membership of Networks:

- Firms Known to DCMS / NCSC
- ADS Group / UK Cyber Security Forum
- Cyber 101 / Bootcamp Attendees
- Cyber Partners
- Cyber Security Suppliers to the UK Government
- Cyber Skills Centre
- CyberExchange
- CyberUK SME Innovation Zone
- CyLon Participants and Alumni
- GCHQ Cyber Invest / Cyber Accelerator
- National Cyber Security Centre Marketplace
- Security Innovation Network (SINET)

Engaged in Cyber Security Sectoral Events / Conferences:

- Firms Known to DCMS / NCSC / DIT through Cyber Security Trade Missions
- Annual Billington CyberSecurity Summit
- Infosecurity Europe Exhibitors

Devolved Regional Analysis:

- Northern Ireland: Consultation with Department for the Economy, and Firms Engaged / Known to CSIT and Invest Northern Ireland
- Scotland: Consultation with Scottish Government (Cyber Resilience)
- Wales: Consultation with Welsh Government (Cyber Resilience) and Identification of North Wales and South Wales Cyber Security Clusters
- UK analysis of clusters (UK Cyber Security Forum's Regional Clusters)
- Firms in Receipt of Innovation Vouchers and / or grants for Cyber Security

9.2 Appendix B: Taxonomy Definitions and Orbis Search Terms

The tables below set out the taxonomy definitions used within this sectoral analysis.

- Information Risk Assessment and Management
- Identification, Authentication and Access Control
- End-User Device Security
- Monitoring, Detection and Analysis
- Incident Response and Management
- SCADA and Information Control Systems
- Training, Awareness and Education
- Cyber Professional Services

This has informed 'key terms' for the long-list identification of firms aligned to trade descriptions. It also serves to inform the extent to which the final list of firms are engaged in particular activities within the cyber security sector.

These have been used for the purpose of this study, and over two hundred potential search terms (below) were tested with DCMS and sector representatives in two workshops. These searches provided over 3,000 potential firms for inclusion in the sector analysis, in addition to the known sources prior to this activity. This meant that firms which were potentially not included or known in existing lists or networks were included in the overall long-list of firms. This long-list was subsequently tested aligned to an agreed scoring criteria (Appendix C).

We recognise that the taxonomy and associated definitions and search terms can be considered subjective, and therefore these parameters were agreed to inform a broad search strategy to capture as many relevant firms as possible prior to inclusion / exclusion in the final dataset.

RSM and DCMS welcome any further feedback on the taxonomy, including definitions and search terms to inform future potential analysis of the sector, and to reflect the potential for change in the nature of cyber security activities.

Information Risk Assessment and Management

Information Risk Assessment and Management	
Definitions	<p>This could look at companies involved in providing products or services aligned to supporting organisations with IT risk assessment and management, with provision of support such as:</p> <p>Implementation of risk and security provision e.g. email filters;</p> <p>Threat, vulnerability and compliance management;</p> <p>Security scanning and testing;</p> <p>Threat and risk detection and response; and</p> <p>Identifying and responding to risks such as malware, ransomware etc.</p>
Key words in ORBIS search: <i>Searches variable: trade description, Products and services</i>	<p>Search for firms with one or more of the following key words;</p> <p>"data security management" , "online security management" , "network security management" , "information security" , "application security" , "intrusion prevention" , "intrusion detection" , "wireless security" , "data risk" , "information risk" , "information security" , "data security" , "ISO 27001" , "GRC" , "GDPR" , "application security" , "DLP" , "security policy management" , "access management" , "cyber threat" , "cyber risk" , "endpoint security" , "security orchestration" , "threat intelligence" , "mobile security" , "risk remediation" , "PSI" , "DCS" , "Cyber Threat Intelligence" , " Certification Body"</p>

Identification, Authentication and Access Control

Identification, Authentication and Access Control

Definitions	<p>Gaining access to computer networks is based on three key steps; identification, authentication and authorisation.</p> <p>Access may be granted through various login credentials including passwords, personal identification numbers (PINs), biometric scans, and physical or electronic keys.</p> <p>This component would cover companies that supply goods or services that control access to computer software or hardware.</p>
Key words in ORBIS search:	<p>Search for the following key term: "security"</p> <p>In addition search for firms with one or more of the following key terms; "virtual identification", "authentication", "access control", "passwords", "personal identification numbers", "biometric", "fingerprint", "electronic key", PKI, "Public Key Infrastructure", "Identity access management", "single sign on", "SSO", "know your customer", "multi-factor authentication", "MFA", "two factor authentication", "authentication tokens", "identity administration"</p>

Network security

Network security

Definitions	<p>Network security refers to any activity designed to protect the usability and integrity of a network and its data. It includes both hardware and software technologies. Effective network security manages access to the network. It targets a variety of threats and stops them from entering or spreading on the network.</p>
Key words in ORBIS search:	<p>Search for one or more of the following key terms: "network security" or "network protection" or "network integrity"</p> <p>"firewall", "security incident event management", "security information and event management", "WAF", "web application firewall", "intrusion prevention", "intrusion security", "penetration testing", "security analytics", "security appliance", "virtual appliance", "MSSP", "managed security service providers", "virtual security service provider", "virtual provider security", "spam filtering", "web application security", "email filtering", "endpoint protection", "encryption", "network architecture", "security operation centre", "network operation centre", "virtual operation centre", "enterprise security", "threat monitoring", "security as a service", "honeynet", "honey net", "vulnerability management", "network analytics", "network sensors", "edge security", "perimeter security", "remote access", "exfiltration", "insider threat", "data loss prevention", "disaster recovery", "Security Architecture", "Cloud Security", "Database Security", "Data Protection", "Encryption", "Internet Security", "Mobile Security", "Secure Information Exchange", "Secure Collaboration", "Secure Hosting", "Removable Media Security", "BYOD Security"</p>

End User Device Security

End User Device Security

Definitions	In information technology, the term end user is used to distinguish the person for whom a hardware or software product is designed from the developers, installers, and servicers of the product. This component looks at firms that allow end users to access or interact with networks using secure devices. E.g. allowing employees to access their companies secure networks using portable devices.
Key words in ORBIS search:	Search key term "security" with one or more of the following key terms also include "end user" , "end-user" , "device" , "user" , "virus" , "threat" , "protection" , "malware" , "end point security" , "end-point security" , "mobile security" "ransomware" , "encryption" , "Secure access" , "zero day" , "phishing" , "trust zone" "patching" , "Cryptography" "code analysis" , "identity access management" , "logical access control" , "user authentication"

Monitoring Detection and Analysis

Monitoring Detection and Analysis

Definitions	This component looks at firms that are involved in the monitoring or detection of varying forms of threats to a network or system. This could include firms that deal with network security monitoring, i.e. the collection, analysis, and escalation of indications and warnings to detect and respond to intrusions. It could also cover firms that provide services in helping other firms to analyse the suitability of their monitoring and threat detection procedures/software/hardware.
Key words in ORBIS search:	"cyber monitoring" , "system monitoring" , "cyber detection" , "system detection" , "online monitoring" , "network monitoring" , "online detection" , "network detection" , "network analysis" , "online threat" , "system threat" , "network threat" , "threat analytics" "threat intelligence" "anomaly detection" "Anomaly behaviour" "botnet" "dark web" "deep web" "Advanced Persistent Threat Detection" , "Security Information and Event Management" , "Security Information & Event Management" , "SIEM" , "Event Monitoring and Surveillance" , "Security Operations Centre" , "Insider Threat Detection" , "Social Engineering Detection" , "Fraud Detection" , "Fraud Prevention" "Intruder Detection Systems" "Red Team" , "Content Monitoring" , "Content Filtering"

Incident Response and Management

Incident Response and Management

Definitions	This component should include firms that deal directly with cyber threats or incidents. This could be either by offering products (hardware or software) to companies or by providing solutions to companies when incidents do occur, e.g. data loss, DDoS attacks or various forms of hacking.
Key words in ORBIS search:	"cyber incident" , "incident response" , "incident management" , "cyber management" , "network incident" , "online response" , "virtual incident" , "virtual management" , "cyber threat" , "online threat" , "online incident" , "cyber issue" , "IT incident" , "IT response" , "security management" , "security response" , "security solution" , "web incident" , "web monitoring" , "web management" , "disaster recovery" , "back-up" , "hacking" "cyber resilience" , "business continuity" "dos" "denial of service" "cyber crime" "cyber-crime" , "advanced persistence threats" "apt" "content delivery networks" , "managed detection" "managed response" "breach detection" "threat detection" "cyber attack" , "cyber-attack" "digital forensic" , "risk remediation" "behaviour detection" "digital rights management" "privileged account management" "access governance" "file analysis" "database encryption" "fraud detection" "forensic analysis" , "Blue Team" , "Digital Forensics" , "Incident Analysis Services" "Cyber Crisis"

SCADA and ICS

SCADA and ICS

Definitions	<p>Supervisory control and data acquisition (SCADA) systems monitor and control critical infrastructures of national importance such as power generation and distribution, water supply, transportation networks, and manufacturing facilities. The pervasiveness, miniaturisations and declining costs of Internet connectivity have transformed these systems from strictly isolated to highly interconnected networks. The connectivity provides immense benefits such as reliability, scalability and remote connectivity, but at the same time exposes an otherwise isolated and secure system, to global cyber security threats.</p> <p>An industrial control system (ICS) is integrated hardware and software designed to monitor and control the operation of machinery and associated devices in industrial environments. Therefore this company should include companies involved in the provision of these products and services.</p>
Key words in ORBIS search:	<p>Search for key word “security”</p> <p>In addition search for one or more of the following key terms; "Supervisory control and data acquisition", "SCADA" , "Industrial Control systems", "ICS" , "programmable logic controller", “utility network” “smart grid</p>

Training, Awareness and Education

Training, Awareness and Education

Definitions	Firms that provide products and services in relation to cyber training, awareness or education.
Key words in ORBIS search:	Search term for all companies including the word “cyber” or “network” in addition to one or more of the following terms “training”, "education" , "awareness" , "crime" , "skills"

Cyber Professional Services

Definitions	<p>Potential to use the definition used by the National Cyber Security Centre:</p> <p>Certified Cyber Consultancies will have demonstrated to NCSC that they have;</p> <ul style="list-style-type: none"> • a proven track record of delivering defined cyber security consultancy services • a level of cyber security expertise supported by professional requirements defined by NCSC • the relevant Certified Professional (CCP) qualifications <p>And that they;</p> <ul style="list-style-type: none"> • Manage consultancy engagements in accordance with industry good practice • Meet NCSC requirements for certified professional cyber services companies • In wider terms this component should include firms that provide professional services or consultancy services (e.g. advice or implementation of solutions) that focus on cyber security.
Key words in ORBIS search:	Search key term “professional services” or with one or more of the following key terms also included “cyber”, “security”, “protection”, “virtual”, “online”, “data”

9.3 Appendix C: Scoring Criteria to Define Firms within Cyber Security

Scoring Criteria	Approach
<p>Criteria 1: Sources</p> <p>Where has the firm been sourced in the initial analysis of sector? (Up to three sources)</p>	<p>Source: (Up to three sources are scored, therefore firms identified in many networks are more likely to receive a higher score)</p> <p>Sourced via an identified cyber network or list (as presented): 2</p> <p>Sourced via ORBIS or Beauhurst or Tracker (not via identified network): 1</p> <p>Sourced via Innovation Vouchers or Other: 0</p> <p>(Max score: 6)</p>
<p>Where firms SIC codes align to Computing Activities (62) and / or security (80), there are considered more likely to be involved in cyber security than other SIC codes.</p>	<p>SIC / NACE Codes</p> <p>Primary NACE code of 62, 80: 1</p> <p>Other NACE code: 0</p> <p>(Max Score: 1)</p> <p>Note this is a low 'max score' given that this analysis does not seek to rely on SIC code analysis as set out in report.</p>
<p>Trade Description/Products and services (Alignment to Taxonomy Terms & Manual Check)</p>	<p>Strong: 3+ matched taxonomy search terms and/or clear alignment of firm's activities (main) to provision of cyber security goods/services Medium: 2 matched and/or some alignment of firm's activities to provision of cyber security goods/services</p> <p>Low: 0-1 matched, and limited alignment of firm activities to provision of cyber security goods/services</p> <p>None: No match, and no obvious alignment (Score = 0) Note that where score = 0, this is subject to validation and has grounds for exclusion</p> <p>Where firms have a:</p> <p>Strong alignment to the taxonomy: Score = 3</p> <p>Medium Alignment to the Taxonomy: Score = 2</p> <p>Low Alignment to the Taxonomy: Score 1</p> <p>No Alignment to the Taxonomy: Score = 0</p>
<p>Scoring</p>	<p>Included / Excluded</p> <p>7 - 10 = Included in Sector Final List</p> <p>2 – 6 = Manual Check (Firms Reviewed and Agreed for Inclusion / Exclusion)</p> <p>0- 1 = Removed from Sectoral Analysis</p>

9.4 Appendix D: Copy of Consultation Topic Guide

[Preamble]

RSM Economic Consulting is currently working in partnership with the Centre for Secure Information Technologies (CSIT) to undertake an important study into the scale of the UK's Cyber Security sector on behalf of the Department for Digital, Culture, Media and Sport. DCMS wishes to understand: the number of UK cyber security companies; the sector's contribution to the UK economy; the number of personnel employed in the sector; the products and services provided; and the sources of funding and investment currently available to support growth in the sector.

The purpose of this consultation would be to discuss with you, your views on the UK Cyber Security sector covering topics such as;

- The current major policy issues affecting the sector;
- Future growth opportunities;
- The current investment and funding landscape;
- Skills and employment in the sector; and
- Any other key areas of interest to you or your organisation

Could I confirm now is still a good time, and that you consent in taking part? Your feedback will be strictly anonymized unless you agree otherwise.

Name:

Role:

Organisation:

Interviewed by:

Date:

Intro and organisation information

Q1. Would you mind telling me about your role, and provide some background about your organisation and its role in the Cyber Security sector?

[May be relevant to ask here for an estimate in % terms (or absolute – e.g. for very large firms) what proportion of their business is related to cyber security]

Q2. [If representative of a company] Within your organisation, what type of cyber security products and /or services do you provide in relation to cyber security and to what extent e.g. focus on software development, hardware solutions, managed services, and or consultancy and training provision?

Q3. As part of this study, we are considering the size and growth potential of cyber security firms against a taxonomy of products and services:

- Information Risk Assessment and Management
- Identification, Authentication and Access Control
- End-User Device Security
- Monitoring, Detection and Analysis
- Incident Response and Management
- SCADA and Information Control Systems
- Training, Awareness and Education
- Cyber Professional Services

In your view, which of these do you feel are best established, or offer significant growth potential for UK firms?

Q4. How many people in your organisation are employed in specific cyber security roles? Within that number, how many would be considered as professional IT staff (e.g. degree or other IT qualification) and how many would be considered to be administrative and or support staff?

Q5. Would you be able to give an indication of the turnover of your organisation (or cyber security department) in the last financial year?

Key policy issues

Q6. The Government published the National Cyber Security Strategy (2016-21) last year and has committed £1.9bn accordingly. One of its main ambitions is to stimulate growth in the cyber security sector, and to measure this against the following outcomes. To what extent do you feel the following are on track to being achieved?

Question	Answer
Greater than average global growth in the size of the UK cyber sector year on year	
A significant increase in investment in early stage companies;	
Adoption of more innovative and effective cyber security technologies in government	
Significantly increased numbers of UK companies successfully commercialising academic cyber research and fewer agreed and identified gaps in the UK's cyber security research capability with effective action to close them	
The UK being regarded as a global leader (economic and leadership) in cyber security research and innovation	

Do you think Government is doing enough to support the emergence and growth of cyber security firms? Are there any other policies/supports you feel would better enable a strong cyber security sector?

Skills, innovation and employment

Q7. What do you view as the main barriers to success in the sector at the moment and how could they be best addressed? E.g. private and/or public investment, skills mix, issues in infrastructure/resources availability, political or economic uncertainty? How can government best support firms to overcome these barriers?


Q8. Do you think the performance of the sector (with regard to developing the necessary skills, growing revenue and increasing employment) will improve, stay the same, or worsen over the next few years (and to what extent)? Are there any particular reasons why you think this to be the case?

Investment and funding landscape

Q9. Have you, or your organisation received any investment in recent years in order to help grow your business [or Cyber security department]?

If so, what forms of support have you been provided with? And how successful do you feel that investment has been?

Do you feel that the type of investment you are seeing now will continue in the coming years?



Q10. Thinking of the support you have had to date (If any), what have some of the tangible/quantifiable outcomes from that investment been? E.g. number of products/new services developed, employment, and improved revenue/profitability

Q11. Any other views?

9.5 Appendix E: Copy of Online Survey

RSM's Economic Consulting team in conjunction with the Centre for Secure Information Technology (CSIT), have been commissioned by DCMS to undertake a UK Cyber Security Sector Analysis exercise to help understand the size, scale and opportunity of the cyber security sector. This review will explore the number of cyber security companies in the UK, and the sector's contribution to the UK economy with regard to revenue, GVA and employment.

Our approach to this review seeks to identify businesses currently developing or selling cyber security products and services, and understand related revenue, GVA and employment as a result of this activity. We are interested in the contribution of these activities within the context of the UK economy.

These activities have been identified utilising a broad cyber security taxonomy in order to capture a wide range of firms in the UK.

In order to inform a wide-reaching and comprehensive study, RSM would greatly appreciate your support in undertaking this short survey (no more than five minutes) to identify the extent to which cyber security represents a commercial component of your organisation.

Please note that any data collected within the survey will be anonymised, and not linked to your business upon publication. Further, this data will only be utilised for purposes of this study for DCMS' understanding of the sector and to inform the development of future cyber security policy and programmes. RSM complies with Market Research Society Code of Conduct, and the Data Protection Act 1998.

If you would like to discuss the survey further, or have any queries or comments, please do not hesitate to get in touch with Project Director Jonathan Hobson (jonathan.hobson@rsmuk.com) or Senior Consultant Sam Donaldson (sam.donaldson@rsmuk.com)

[Consent Field]

Q1a. Which organisation do you work for / are submitting this survey on behalf of?

[Open Text]

Q1b. What is your current position within the organisation?

[Open Text]

Q1c. Email Address (not used for any purpose other than clarification)

[Open Text]

Q2. Could you provide the full registered trading name of your organisation?

[Open Text]

Q3. Could you provide, where possible, an estimate of your organisation's:

- Revenue in the UK in most recent available year e.g. 2015/16 (state yyyy)
- Employment (FTE) in the UK in most recent available year

Q4. Which of the following cyber security (taxonomy related) products and services (if any) does your organisation provide?

[List of Product and Service Activities – using taxonomy headings]

Q5. As part of this study, we are seeking to understand the extent which cyber security activities represent part of your firm's economic activity. [Of those selected], what number (or proportion) of your organisation's revenue/employment would you estimate to be within each product and or service line?

[List of Activities + Space for Insertion of Absolute Revenue and Employment related to cyber + Field for Raw Data + Comment Box]

Q6. Of the cyber security activities you have identified, what proportion of these would you estimate to take place in the following UK regions?

[List of 12 regions + proportion field]

Q7. Where staff within your organisation are employed for the development of cyber security products or services, could you provide an estimate of:

- Average Remuneration
- Median Remuneration
- Remuneration Range by Experience (Graduate/Junior, Senior (3-7+ , Principal 7+, Director 10+, Partner/CEO)

Q8. We are also interested in understanding the skills and labour available to the cyber security sector. Do you have any views on the current state of skills and talent available to the cyber security sector within the labour market?

[Open Text]

Close Survey.

9.6 Appendix F: Investment Funding Definitions

Seed Funding

Seed capital is the initial capital used when starting a business, often coming from the founders' personal assets, friends or family, for covering initial operating expenses and attracting venture capitalists. This type of funding is often obtained in exchange for an equity stake in the enterprise, although with less formal contractual overhead than standard equity financing. Seed funding concentrates on the very early stages of young innovative companies which are characterised by high level of investment risk. It is aimed at supporting companies to move away from the prototype stage to commercial revenue. Because banks and venture capital investors view seed capital as an "at risk" investment by the promoters of a new venture, capital providers may wait until a business is more established before making larger investments of venture capital funding.

Within the UK, 40% of businesses last year required less than £10,000 and two thirds required under £100,000.⁸⁹

Venture Funding

Venture Capital (VC) funding is a specific type of finance suited for the requirements of new technology based firms. These investments are generally characterized as high-risk/high-return opportunities. The combination of research and development, intangible assets, negative earnings, uncertain prospects and absence of a proven track record, which are characteristic of start-up and pre-commercial initiatives, leads to an unacceptably high perception of risk for conventional financial institutions and debt financing. Venture capital addresses the consequent financing gap through equity participation.

A typical VC investment will be £250,000 or over.⁹⁰

Growth Investment

Growth investment involves investing in the shares of a company whose profits have grown strongly in the past and are expected to keep on doing so in the future or at least where turnover is expected to grow rapidly and profits will follow. Unlike the shares favoured by value investors, growth shares tend to have high PE ratios and pay very small or no dividends. They are more commonly associated with smaller rather than larger companies.

Growth investment is usually between £2m and £10m, and may encompass a minority equity stake and board seat.⁹¹

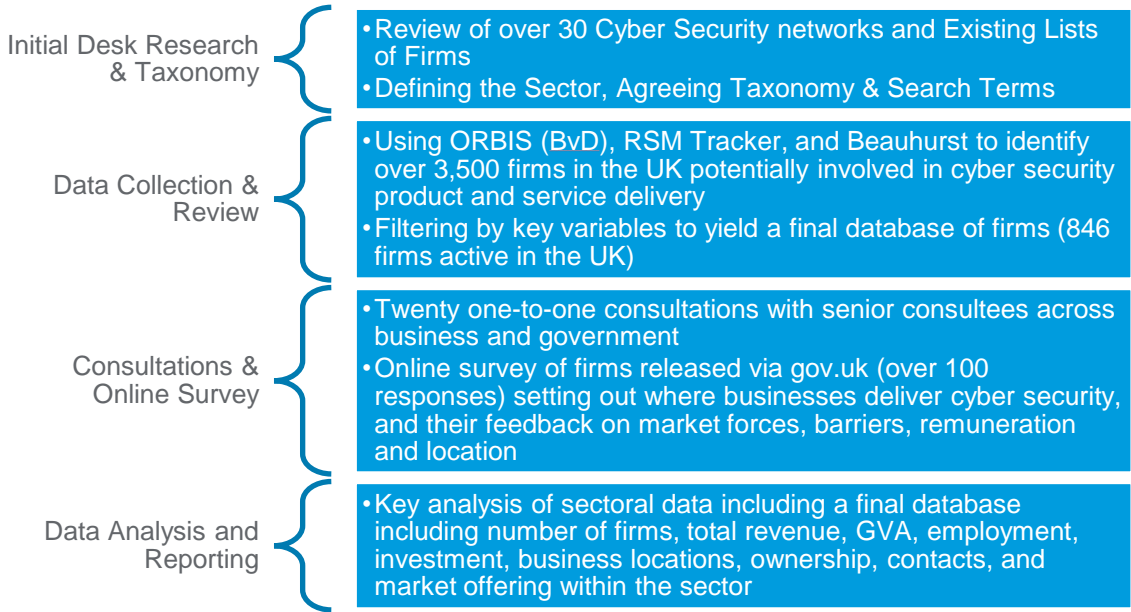
⁸⁹ <https://www.angelinvestmentnetwork.co.uk/funding-startups>

⁹⁰ Ulster University, *Funding Guide for SMEs*. Available at:

https://www.ulster.ac.uk/__data/assets/pdf_file/0007/69370/sme-funding-guide.pdf

⁹¹ <http://www.businessgrowthfund.co.uk/what-is-growth-capital/>

9.7 Appendix G: RSM Research Methodology



This study adopts a ‘bottom-up’ approach to identifying economic activity within the UK Cyber Security sector. It recognises the challenges associated with a ‘top-down approach’ e.g. using SIC codes, which may fail to capture emerging firms within UK cyber security, as well as firms which provide a significant volume of cyber security goods or services, but may not typically be considered as a ‘cyber security firm’ e.g. providers of consultancy services. A wide range of data sources were used to inform the study. These include:

Primary Data	Secondary Data	Consultations & Research
<ul style="list-style-type: none"> • Access to over thirty identified networks, clusters and events (listing known cyber security firms, or firms engaged with cyber security sector) • Access to LinkedIn (for real-time identification of firms in 2017, and to inform a profile of firm’s activities and employment by region). 	<ul style="list-style-type: none"> • Orbis (Bureau van Dijk) to collate Companies House data and statements (over 11m UK companies) • RSM Tracker (similar to Orbis, in-house). This provides insight into company turnover, GVA, gross profits, employee remuneration, and location of firms • Beauhurst, a leading investment analysis platform. 	<ul style="list-style-type: none"> • Approx. 20 one-to-one consultations with leading representatives in the sector from industry, government (national/devolved), and academic partners; • An online survey, promoted by DCMS in August 2017, to collect further data on cyber security activity in the UK

A combination of these sources was used to identify cyber security firms in the UK. These firms were collected through identified networks and clusters, in addition to key search terms input into Orbis and Tracker to identify cyber security firms which may report activities within their trade description, but may not be part of an existing network. The database has been tested against the taxonomy of cyber security firms, and each identified firm has been scored to determine sector relevance.

Primary Research

RSM conducted two forms of primary research for this report. This included in-depth telephone interviews with twenty cyber security sector stakeholders to obtain in-depth views of the economic contribution and performance of the cyber security sector, and views on how the sector might be best supported by

government. These stakeholders included a broad range of industry subsectors and government departments, across all UK regions.

In addition, an online survey invited individual firms to provide their own data regarding the extent to which cyber security products and services contributed to their firm's revenue and employment, and to provide the regional breakdown of their firm's employment and associated employee remuneration. This was publicised via DCMS, the gov.uk website, social media, and several cyber security networks such as ADS, CyberExchange, and CSIT in August 2017. In total, 107 usable responses⁹² were received.

Defining the sector and identifying businesses / Establishing a long-list of businesses:

The study drew upon a range of sector expertise to identify a list of key search terms for each component within the DCMS Cyber Security taxonomy. On this basis, the analysis could therefore be further refined in the future subject to any changes in the definition or areas of interest within the Cyber Security taxonomy.

The search terms were subsequently used within Bureau van Dijk's Orbis platform to identify an initial long-list of firms which should be examined as to whether these were to be included in the final dataset i.e. that they were clearly providing cyber security products and services within the UK. Over two hundred search terms across the taxonomy were explored in the initial identification of potential cyber security firms.

An initial list of over 2,500 firms in the UK was identified using the key search terms in Orbis at the initial research stage. This list of firms was subsequently added to the list of firms identified from source lists provided by DCMS and CSIT (firms known to have been involved in cyber security activity, exhibitions, forums or the Cyber Essentials scheme). Following the removal of 'duplicates', the initial Orbis search and list of known businesses active in the UK provided a long-list of approximately 3,500 firms for subsequent analysis and testing.

Interim list of cyber security businesses:

The initial long-list of cyber security businesses was refined using a scoring mechanism to exclude firms that were not deemed relevant to the cyber security sector. The scoring system used a range of weighted fields including identified sources, SIC code, trade description, and product and service description to produce a score of between 0 and 10 for each firm. Firms scoring 0 - 1 were removed, those with scores of between 2 - 6 were manually reviewed by sector experts for inclusion or exclusion, and firms with scores of 7 - 10 were automatically included.⁹³

Based on this approach, the number of firms included in the final analysis was refined to 846.

Approach to Analysis and Reporting

This sectoral analysis follows an experimental approach recognising the limitations in identifying cyber security revenues, employment and GVA using a traditional SIC code approach. As a result, RSM has utilised a number of data sources as well as methodological assumptions to inform the analysis, and provide an overview of the sector.

Following the identification of the short-list of firms, it was important to identify the subsequent constraints of the data available, and to provide clear assumptions to address gaps in data. This stage provided three key research challenges:

1. **Where companies are considered micro or small⁹⁴, firms are only required to provide abbreviated accounts to Companies House.** This means that revenue and employment statistics may not be available. Of the 846 firms identified, 576 (68%) of these did not provide such data to

⁹² Other responses were excluded where most answers were not complete or the respondent did not complete the survey.

⁹³ Note that in some cases firms with a score of 0-2 or 7-10 were manually reviewed if deemed appropriate by the research team e.g. where a firm was identified in many sources, but could not be considered for inclusion due to limited taxonomy alignment.

⁹⁴ A company will be 'small' where it has any two of the following conditions: a) a turnover of £10.2m or less b) £5.1m or less on the balance sheet c) has fewer than 50 employees.

Companies House. Therefore, these firms required estimation and or desk review to establish a more robust overview of their activities and extent of operations.

RSM therefore undertook desk review of all 846 firms, using where possible (by order of preference):

- **Provided firms the opportunity to report** their own revenue, employment and products and services (as a wider firm, and from cyber security products and services) through one-to-one consultation and the online survey;
 - **Company Annual Reports and online information** to validate their known trade description, products and services, and associated employment and revenue;
 - **Company Profiles on LinkedIn⁹⁵**: This explored staff reported employment with firms (in the UK, and filtered where appropriate by suitable category to filter by staff most likely to be involved in Cyber Security divisions within firms that provide cyber security products and services). This was particularly key to estimating employment in micro firms. Where a small UK cyber security consultancy has limited information via Companies House but has six current employees on LinkedIn, for example, this was used to provide a rounded estimate by each firm.
2. It is recognised that it is **not appropriate to allocate all revenue or employment figures to the sector** of the firms identified where they provide multiple services, as this would provide an over-estimation of the extent to which revenue and employment is attributable to the sale of cyber security products and services. This raised the challenge of identifying where firms are either:
- **'Fully Dedicated'** i.e. all (100%) of their revenues and employment can be attributed to provision of cyber security products and services;
 - **'Mostly Dedicated'** i.e. more than 75%⁹⁶ of their revenues and employment can be attributed to provision of cyber security products and services; or
 - **'Diversified'** i.e. less than 75% of their revenues and employment can be attributed to provision of cyber security products and services.

The extent to which firms were identified as 'dedicated' or 'diversified' was subject to where cyber security employment represented a percentage of the firm's total employment. In other firms, where a firm has twenty employees, that were working to provide cyber security products and services, this firm was considered fully dedicated.

Where a typically larger firm reported that, for example, 500 of their staff (out of a total of 20,000 staff) were working to provide cyber security products and services, this firm would be considered 'diversified'.

In the online survey undertaken in August 2017, firms were asked the extent to which their firm's revenue and employment was attributable to cyber security products and services. Firms reported that the relationship between percentage of revenue and percentage of employment was comparable i.e. where cyber security revenue was 60% of all revenues, cyber security employment would reflect 60% of all firm employment. This builds the assumption into our analysis that the relationship between a firm's revenue and employment is linear.

⁹⁵ Recognising the potential for 'under-reporting' in LinkedIn due to coverage of accounts; set out in Section 3.3.

⁹⁶ The figure of 75% is used as an RSM assumed cut-off for dedicated/diversified as it is assumed that where firms are diversified, they may still be 'operational' without providing cyber security products or services. This is for research and analysis purposes only to understand how many firms **only** provide cyber security products and services, and their respective contribution to the sector and wider economy.

Addressing 'gaps' in data identified

It is recognised that given the nature of the firms, and reporting requirements, that gaps exist in the official financial reporting of firms (particularly due to abbreviated accounts). Therefore, we set out the approach to estimating sector variables where gaps exist.

Variable	Approach to Gaps
<p>Size of Firm: All the 846 firms are known by 'size' i.e. large, medium, small and micro (see Section 3.2).</p>	<p>There were no gaps in this data. This meant that the parameters of each firm were known (see Table 3.1). This allowed RSM to identify average and median values of known data, and to use this where appropriate to inform estimates of revenue and GVA for firms with gaps.</p>
<p>Employment: RSM undertook desk research into all firms separately (including consultation, desk review and LinkedIn) to estimate each firm's employment.</p>	<p>As RSM estimated each firm's employment and built upon existing databases, this provided an overall employment estimate of the sector and each firm.</p>
<p>Revenue: In addition to use of Companies House data, RSM segmented firms by size to understand estimated typical revenue of firms not required to report revenue based on wider sector performance.</p>	<p>Where employment was known in firms, but revenue was a gap, RSM examined firms (by size) with known revenue and employment data. This provided an estimate of average and median revenue by size of firm. This was used to inform revenue gaps where employment was known e.g. where typical revenue for a micro firm was, for example, £35,000 and this firm had 5 employees, then estimated revenue would be £175,000.</p>
<p>Gross Value Added (GVA): $GVA = \text{Operating profit} + \text{Employee Costs} + \text{Depreciation \& Amortisation}$</p> <p>Where available with Orbis and Tracker, RSM totalled GVA for known firms.</p>	<p>Where GVA was known at the firm level (for c. 270 firms), this provided a known ratio of GVA-to-Revenue within firm by size e.g. 0.4: 1. This informed GVA by firm size where operating profit, employee costs, depreciation and or amortisation were unknown. This was estimated for all gaps, and a total GVA figure is provided in this analysis.</p>