Lancaster University

# The North West Cyber Security Industry
# Export Potential Assessment

# Foreword

Foreword can go here

## Contents

Introduction ..... 1

Methodology..... 3

Demographic Information ..... 10

Cyber Security Activities & Capabilities..... 18

Export Activity and Potential..... 25

Collaboration..... 37

Case Studies ..... 40

Conclusions ..... 50

Appendix 1 ..... 52

Appendix 2 ..... 54

Appendix 3 ..... 55

Appendix 4 ..... 56

# Introduction

Cyber Security businesses in the North West of England form an industry which is growing. This study has taken an in depth analysis of the industry to determine its size, make up and readiness to export and is the first of its kind classifying business within the framework identified by the UKTI cyber export strategy. This report presents the findings of the research undertaken independently by Lancaster University commissioned by the UKTI.

Cyber Security was categorised by the 2010 UK Strategic Defence and Security Review as is a tier one UK security threat. It is expected to continue to be a high priority in the outcome of the next strategic review. The connectivity which enabled networked business, cultural exchange and social change also facilitate new kinds of threats and accidents. Computer systems control many aspects of our daily lives from public infrastructure such as roads and buildings to our personal data including health and communication records. Furthermore computer systems underpin business both in the UK and Internationally. These systems include hardware (including networks, computers, mobile devices, machinery etc), software (including operating systems, security software, application, updates etc), information (including data, usage policy, security policy, legal stipulations etc) and people (to create, maintain, operate and benefit from the systems).

Cyber security consists of the products and services which attempt to secure the vulnerabilities native to networked communication. Products include hardware such as firewalls and backup servers and software such as anti-virus detection software and forensic software. Services include ongoing system support in the form of crisis management or system surveillance or analysis of large quantities of data. The reputation of the UK in terms of cyber security capability is very high with the UK recognised as the leading G20 nation as ranked by the 2012 Booz Allen Hamilton cyber power index[1]. As such the technologies and skills available in the UK are highly sought after globally. For this reason the UKTI cyber export strategy[2] was designed to promote the UK capability into the estimated £123bn global cyber security market. In 2013 the UK export market for cyber security products and services was estimated to be £805m, 33% of the total UK security exports with figures published by the UKTI in 2014 that the exports had passed £1bn with the expected target of £2bn worth of exports by 2016.

The North West of England is a largely rural region of the UK. However the region houses large and innovative businesses especially in Greater Manchester and the Liverpool area. The region is also home to several research universities (Lancaster University, The University of Manchester & The University of Liverpool especially) who add value to the regional economy directly and through the development of skilled workers. Specifically Lancaster University is recognised by the EPSRC and GCHQ as an Academic Centre of Excellence in Cyber Security Research (ACE-CSR) and is one of only four national institutions with its masters degree programme in cyber security accredited by GCHQ. Lancaster has used its academic position as a leading anchor institution in the North West to

[1] http://www.boozallen.com/media/file/Cyber_Power_Index_Findings_and_Methodology.pdf

[2] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/275566/UKTI_Cyber_Security_Brochure.pdf

stimulate the cyber security industry, working directly with large and small companies, along with supporting initiatives such as the North West Cyber Security Cluster.

This report sought specifically to understand the ability of The North West Cyber Security Industry to export. This involved an exploration of the current export levels within the industry and the reasoning behind export decisions. From the research undertaken It can be identified that the North West cyber security industry is composed of mainly small to medium sized enterprises turning over on average £50k to £250k p.a. In total 120 companies were identified as offering cyber security products or services employing around 1000 people providing a regional industry worth £355m in turnover p.a.. The majority of the businesses are service based companies with a smaller number of product development or system integration companies.

From the analysis of the data, around one third of the companies are already exporting into many of the key markets identified by the UKTI strategy with the US and EU countries providing the primary export destinations. Further, those companies that are exporting are looking to expand into other new markets outside of English speaking countries. There is some enthusiasm from the remain companies to undertake an export approach, however, concerns around the nature of the products, for example dual use issues, and expertise in the markets, and company size and capital to expand into new markets are holding companies back from dipping their toe into the exports market.

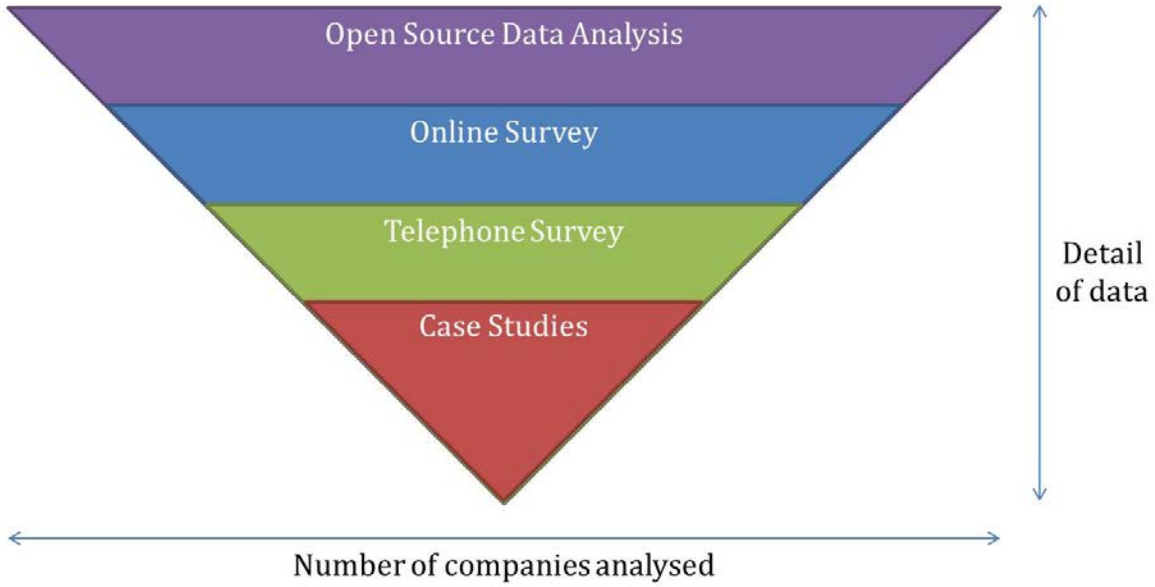
There are two elements to progressing cyber exports from the North West. Firstly the North West cyber security industry is small, young but growing fast. Given this make up many of the companies will not be ready to export or, have even considered exporting as they cope with their rapid expansion. With these companies it will be important for the UKTI to work with them to integrate exporting as part of their growth plan early on, helping them to recognise when the time is right to start exporting and then support them in their endeavours. Secondly, with a third of companies already exporting there is an opportunity to identify “role models” and mentors to advocate the exporting approach. Key lessons can be learnt from these companies in how they broke into the geographical markets they operate in. Further, those exporting companies predominately export to English speaking nations due to language lowering the entry barrier. Support here must focus on how to enter the priority markets highlighted in the export strategy, and overcoming the perception that entry into those markets may taint their existing export customers.

Beyond this a focus should be made to align the export approach to the key industries based in, and associated with the North West, such as Energy production, utility distribution, advanced manufacturing, health and financial and professional services. Building a reputation within any of the industrial segments for cyber security will enable the North West to compete with other regions, particularly southern regions which are known for the defence and intelligence sectors. Reputation building on a global stage for these key sectors will increase the demand as those industries identified increase their security spend, for example the market for industrial control system security which will be crucial to manufacturing, energy and utilities is expected to grow to $11.29bn in 2019 from $7.82bn in 2014 according to Markets and Markets report[3].

[3] http://www.marketsandmarkets.com/PressReleases/industrial-control-systems-security-ics.asp

# Methodology

The objective of this study was to both identify and analyse the North West Cyber Security Industry and the industry's ability to export. A funnelling model of data collection was used which started with a wide analysis of the market and result in a deep understanding of individual companies. This methodology involved drawing on open source data sets for broad market identification and then utilised telephone/online surveys and finally interviews to provide case studies.




## Open Source Data Collation

### Identification

The first stage of research involved synthesising open source data to identify a representative set of businesses in the North West of England that could be classified as Cyber Security companies. Sources of information used were: search engines (Google and Yell), public lists of qualified individuals (for example LinkedIn profiles or CESG qualified personnel lists), lists of companies accredited to provide key cyber security services (i.e. ISO27001, CREST). This investigation created a set of potential candidate companies about who little was known. During the identification phase a key issue was identified which hindered the process. There is no central mechanism to identify a company as cyber security as there is with other industries through the utilisation of Standard Industrial Classification (SIC) codes.

In order to create a list of companies who could be considered to be representative of the North West Cyber Security Industry each candidate company required inspection. The online presence of each company was utilised to gain further insight. This presents a problem because some businesses utilise their website well while others may not promote themselves via the Internet.

The criteria which companies needed to meet in order to be considered part of the North West Cyber Security Industry were:

- A main office, or significant business unit, located within the National Office of Statistics designated North West England regional postcodes. [4]
- Must take part in at least one of the nine UKTI cyber security activities outlined in the UKTI export strategy.[5]
- Business must be active according to Companies House data. (Sole traders/partnerships were contacted direct to clarify activity status).

Based on these criteria there are some omissions which should be discussed.

While global players such as BAE Systems operate within the North West and in fact have a significant cyber capability to protect their business assets located there, they were discounted as their main business unit supplying cyber security products and services, Applied Intelligence, is based outside the North West. In comparison Fujitsu is included within the data set as they have a business unit based in Warrington that supplies cyber security products and services. Where there is a lack of clarity regarding the level of cyber security work done in the region, as is the case with KPMG based in Manchester, they have not been included. As a result some large organisations that are extremely important players are not included within the data, however, they have highly strategic and important role in the regional cyber security business ecosystem.

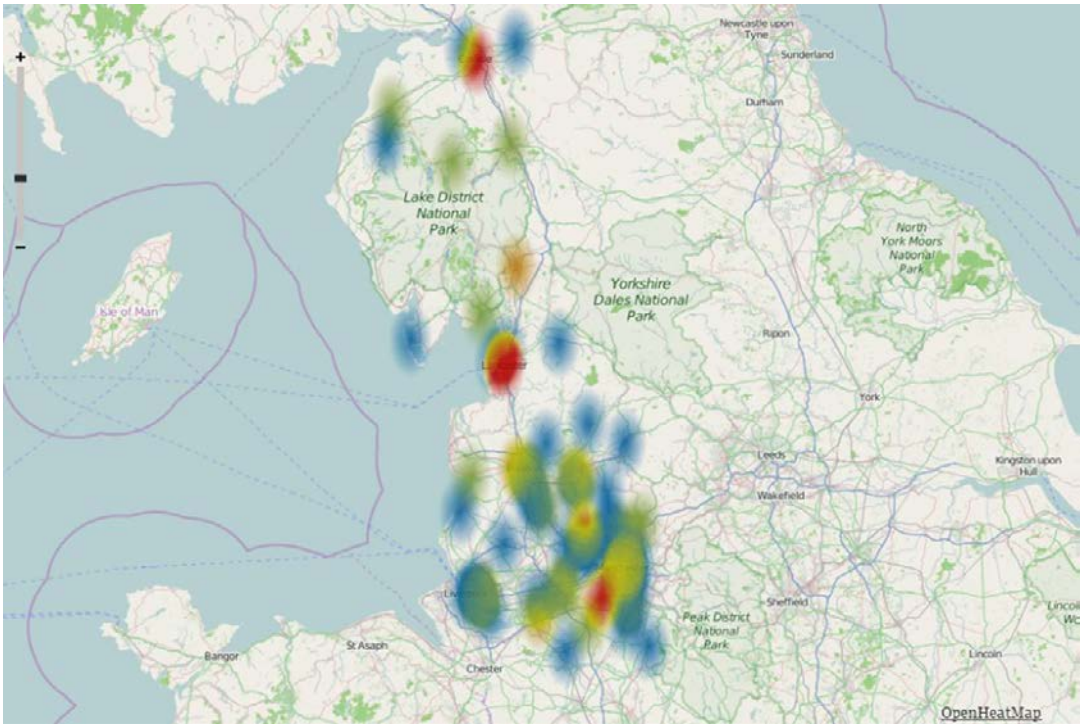
Other business types were identified but rejected at the identification phase because they did not fit in the UKTI cyber security activity criteria. Business types rejected because they do not fall in to the UKTI cyber security activities profile include law firms dealing with cyber activities and insurance companies with an interest in cyber security insurance.

The identification phase resulted in a list of 120 companies who fulfilled all of the above criteria.

[4] ONS. *Regions and their Constituent Counties and LADs in the UK as at Dec 2011*. (2011). Available at: https://geoportal.statistics.gov.uk/Docs/Maps/Regions_and_their_constituent_counties_unitary_authorities_(UK)_Apr_2011_map.zip

[5] UKTI. *Cyber Security: The UK's approach to export*. (Crown: London, 2013): p. 7

**Distribution of cyber security industry within the North West of England (Blue = Lower Concentration, Red = Higher Concentration)**




## Company Demographic Information

The body of data identifying companies was compared against company registration information held by UK Gov Companies House and maintained by DueDill. This data was used to gather demographic information. Information gathered from these sources included:

- SIC Codes (2003 & 2007)
- Turnover
- Company Size (Employee numbers)
- Company lifetime.

In regard to the company turnover, many SMEs are only required to file abbreviated company accounts which do not include details of turnover. In these instances an estimating calculation was used to identify ranges of turnover. This calculation estimated turnover based on Trade debtors, assuming a usual trade credit period of 60 days. In this instance the estimated turnover calculation used was:

Current Debtor amount/60 = Turnover per day.

Turnover per day x 365 = Estimated Turnover (year)

Demographic information on a total of 26 companies within this final data set could not be identified. This was due to the companies acting as a sole trader, a status that does not require company registration. Between sole traders and incomplete public accounts complete economic records were somewhat rare. However, such a sample sizes provides confidence in calculations relating to the growth rate of the industry and how capable the industry may be in exports in the future.

## Website Analysis

With 120 companies identified an examination of the publically available information on the operation of the company from the website undertaken to identify:

- Cyber Security Capabilities
- UKTI Cyber Security Segments
- Export Readiness

### Cyber Security Capabilities

In order to be considered for study the companies had to be active in at least one of the nine cyber security activities identified by UKTI. The process by which companies were identified is outlined in Appendix 1. The company's operations in each of these activities were also broken down into four capabilities. An explanation of these capabilities and the process by which we assessed the companies can be found in Appendix 2. These classifications included: Service Provision, Product(s), Integration and Design.

### UKTI Cyber Security Segments

The UKTI segment the Cyber Security Industry into three parts:

- Advisory work (Devise security policies, strategies and management/audit methodologies)
- Assurance work (Validates, verifies and characterises parts or whole of a capability)
- Education work (Builds knowledge, skills and know-how)

Based on evidence present on company websites the company was categorised into one or more of these segments.

### Indicators of Export Readiness or Current Activity

Website analysis provided a limited opportunity to also collect indicators regarding a company's readiness or current activity to export their products/services to overseas markets. For example if a company explicitly described itself as being:

> *"…happy to provide free quotes and advice to new and existing customers across Liverpool"*[6]

Or if the company was clearly focused on business within a small area of the region, with no reference what so ever to international business (e.g. blog posts, case studies or testimonials) then it was considered that the business is unlikely to export and had no plans to export in the near future. Based on this examination companies were ranked as unlikely, possible, highly likely or unknown at this stage with the intention that the latter survey stages would be undertaken to verify this information. Data was recorded regarding all 120 companies on:

- Cyber Security Capabilities
- UKTI Cyber Security Segments

The data collected provided a straight forward, simple and quick approach to assessing the activities, capabilities and segmentation of companies in the North West providing a core data set central to this study. Collecting information about export readiness using this method allowed us to capture data points which may have been otherwise missed. However it should be worth note that the data

[6] The Computer Doctor Liverpool. Home Page. Available at: http://www.liverpoolcomputerdoctor.co.uk/

collected here is only as accurate as the websites on which it is based. For this reason all of the companies were asked to verify this information through the online and telephone surveys

# Direct Questioning

In order to gather further detailed information regarding the identified companies in the previous section, and also potentially identify companies that may have been missed, an online and telephone survey was conducted. Broadly the online survey was undertaken to; broaden and identify other possible companies, to gain higher resolution on demographic information and to understand more fully the export capacity, activity and readiness of the companies. The Telephone survey was utilised to identify further information regarding the export capacity, activity and readiness and also identify potential companies for case studies. Combining the online survey responses and the telephone interviews export information for 22.5% of the total companies identified was obtained. This is considered to be a representative data set for the overall population and so it is possible to extrapolate within reason to the whole population.

## Online Survey

Data collected in this phase was collected to help identify areas such as perceptions of important growth factors and perceptions of export capabilities along with further data on company demographics. The survey was sent out to all 120 companies who form the core of this study. This was achieved through direct mailing through known email addresses. In addition we sent the survey to all of those companies who were originally identified as candidates for the study but were rejected for not fulfilling the prerequisite criteria for this study (this was in order to ensure that we were correct to reject those companies). Finally we used internal and third part distribution channels to give as many companies in the North West of England the opportunity to take part in the online survey. Third party distributors included:

- Creative Lancashire
- East Lancashire Chamber of Commerce
- Greater Manchester Chamber of Commerce
- Halton Chamber of Commerce
- Lancaster Chamber of Commerce
- Liverpool Vision
- South Cheshire Chamber of Commerce and Industry
- St Helens Chamber of Commerce

Each of these distributors used social media, their website, newsletter, e-bulletins and/or advertisements within membership areas to distribute a web link and short text explanation of the purpose of the survey to their members or customers. As a result there is no clear data to suggest the ultimate reach of this campaign but for some context Greater Manchester Chamber of Commerce's newsletter reaches more than 6,000 businesses located within Greater Manchester. In order to incentivise the completion of the survey a Kindle Fire tablet was offered as a prize for one randomly selected individual who completed the survey. The survey consisted of 32 questions which aimed to collect data about company demographic, activity/capability, market perceptions, export activity, export readiness and engagement with external organisations (such as government agencies and overseas institutions). A copy of the Online Survey can be found in Appendix 3.

The online survey achieved 38 responses of which 17 were complete with the remaining responses were rejected for the following reasons.

| Number of Rejections | Reason for Rejection |
|---|---|
| 10 | Declined to answer any questions |
| 3 | Refused data policy outlined at the start of the survey |
| 3 | Supplied Demographic Data only |
| 3 | Located outside of North West England |
| 1 | Spoiled Survey |
| 1 | Not a cyber-security company |

Therefore 11.7 % of the 120 companies identified as being part of the North West Cyber Security Industry are represented in this online survey. This return rate is typical of return rates found in the marketing industry of around 10-15% for external surveys[7].

The online survey allowed us to gather data on representative companies and improved the accuracy of our overall picture of the North West cyber security industry. This information validated our turnover estimates and also provided a valuable insight into the industry and its export capability. A higher response rate would have been preferred, however, despite providing an incentive, it is likely that the focus on export of products and services did not resonate with the target group as they did not self-identify as exporters. Anecdotally, this played out in the discussions held as part of the interview and case study process.

### Telephone Survey

To generate a higher resolution a telephone survey was undertaken with those companies that had not responded to the online survey. The questions asked were the same as those from the online survey but with much more focus on the export section. The questions asked can be found in Appendix 4. 13 companies responded to the telephone interview, 10.8% of the 120 companies identified. This response rate is in line with previously referenced industry standards**.** Short telephone interviews were also used to identity sole traders and further cleanse the original set of company data in order to get better accuracy on economically active companies. Many companies who declined to speak to us did so because they did not have time for the call (they did not consider the call a priority) or they had a strict “no telephone survey” policy this was certainly the case with the larger more established companies.

## Case Studies

To understand more fully the role exports play in the cyber security industry in the North West, it was decided to undertake a series of unstructured interviews with exemplar companies which responded either to the telephone or online survey. Based on the analysis for the data from the

[7] Survey Gizmo. *Survey Response Rates*. (January 2010) Available at: http://www.surveygizmo.co.uk/survey-blog/survey-response-rates/

direct question phase three classes of company in relation to their attitudes to export were identified. These categories are:

- Those who do not export and have no desire to export – Computer Doctor Liverpool
- Those who do not export but desire to export - MDSec
- Those who do export – NCC Group

These case studies offer a much deeper and richer picture of the positions these companies find themselves in and allow us to draw distinctions between those who currently export and those who do not and those who wish to export and those who do not. However it is not possible to draw conclusions which encapsulate an entire group within the North West Cyber Security Industry based on the experience of a single company. There may be further conclusions to draw from further case studies. Also, these case studies drew upon an interview with a single individual within the organisation. A more inclusive methodology would yield more reliable conclusions given more time.

# Demographic Information

Demographic research paints a picture of a developing industry driven by independent entrepreneurs with sustained interest from large multinational organisations. The data presented here demonstrates that the North West Cyber Security Industry has developed out of a diverse range of business activities. Sales within the industry range dramatically with 15% of companies turning over less than £50,000 last year and 20% of companies turning over more than £40 million. There is more uniformity regarding company size as the vast majority of companies in the industry can be considered Small Enterprises. The industry is young and growing. However the lack of a Medium Enterprises sector is a significant concern.

## SIC Codes

No single SIC code describes cyber security companies. As such the data collected from DueDil about cyber security companies in the North West paints a diverse picture. SIC 2007 codes were collected for all of the companies who supplied them to Companies House. This resulted in data from 73 companies (60.8% of the industry) spanning 20 different SIC Codes.

**Table 1 list of SIC 2007 codes used by North West Cyber Security Companies**

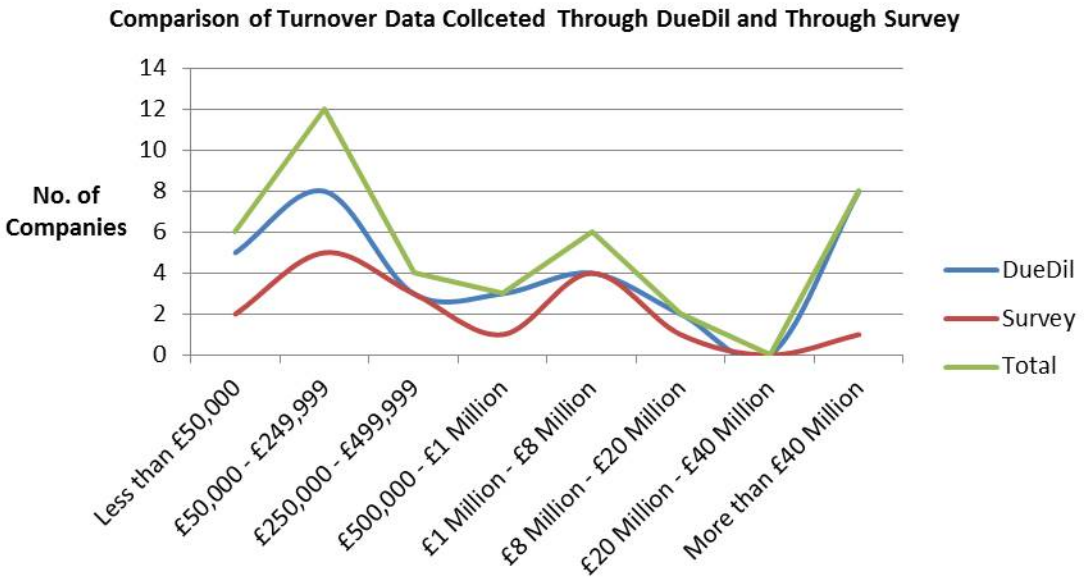
| SIC 2007 | No. of Companies using code |
|---|---|
| 62020 — Computer Consultancy Activities | 29 |
| 62090 — Other Information Technology And Computer Service Activities | 14 |
| 62012 — Business And Domestic Software Development | 6 |
| 82990 — Other Business Support Service Activities N.e.c. | 4 |
| 74909 — Other Professional, Scientific And Technical Activities (Not Including Environmental Consultancy Or Quantity Surveying) N.e.c. | 3 |
| 61100 — Wired Telecommunications Activities | 2 |
| 61900 — Other Telecommunications Activities | 2 |
| 26110 — Manufacture Of Electronic Components | 1 |
| 46510 — Wholesale Of Computers, Computer Peripheral Equipment And Software | 1 |
| 47410 — Retail Sale Of Computers, Peripheral Units And Software In Specialised Stores | 1 |
| 63110 — Data Processing, Hosting And Related Activities | 1 |
| 64209 — Activities Of Other Holding Companies (Not Including Agricultural, Production, Construction, Distribution And Financial Services Holding Companies) N.e.c. | 1 |
| 65120 — Non-Life Insurance | 1 |
| 73110 — Advertising Agencies | 1 |
| 73120 — Media Representation | 1 |
| 70229 - Management consultancy activities other than financial management | 1 |
| 78200 — Temporary Employment Agency Activities | 1 |
| 80300 — Investigation Activities | 1 |
| 95110 — Repair Of Computers And Peripheral Equipment | 1 |
| 96090 — Other Personal Service Activities N.e.c. | 1 |

This list includes business activities which may be surprising. While "62020 – Computer Consultancy Activities" would be an expected code to be used by those who are active in cyber security, codes such as "65120 – Non-Life Insurance" were harder to predict. Clearly the more surprising codes are used less by North West Cyber Security companies. Use of these codes can be attributed to diversification into cyber security activities from other core activity. It is important to note that such a diverse range of SIC 2007 Codes suggests that support for cyber security companies could involve supporting companies based in industries beyond the recognised computing and technology industries into marketing, insurance and general business support.

This list is representative of the SIC Codes used by North West Cyber Security Companies. 46 cyber security companies in the North West (38.3% of the industry) do not supply SIC codes to Companies House either because they are not required to (e.g. Deloitte) or because they are sole traders (e.g. AG Constancy).

# Turnover

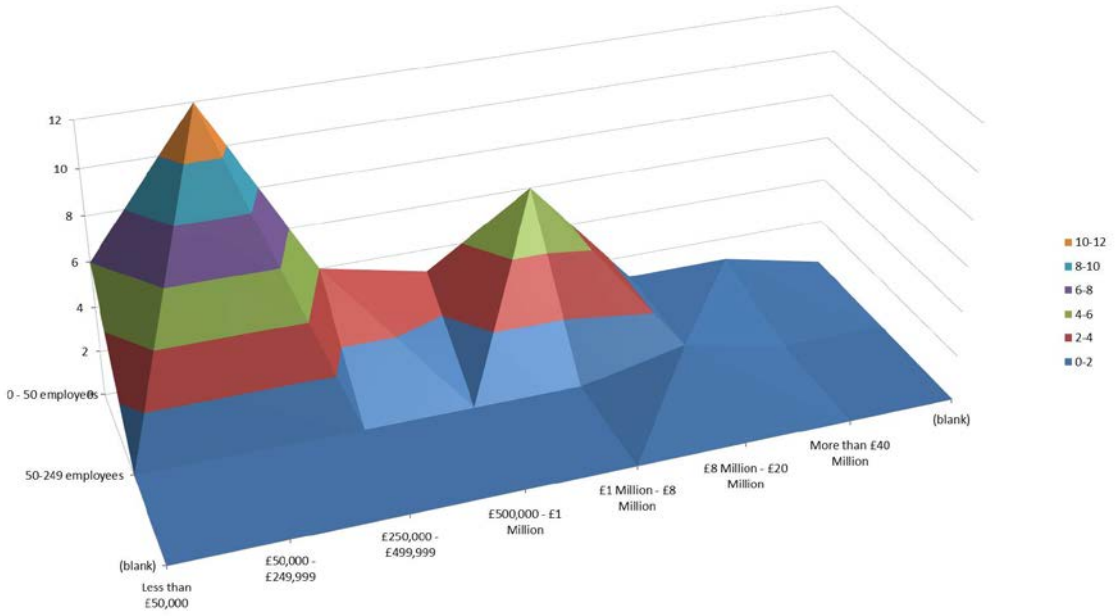
The turnover of North West Cyber Security Companies ranges greatly. As presented in the methodology data was collected from surveying (17 companies) and from open source data sets (33 companies). Comparing the gather data, it can be seen in the graph below that the information from the survey is representative of the data set gathered from the open source information. These To combine the data sets together data was selected based on the following preference criteria, companies house reported turnover, self-reported survey turnover answer, estimated turnover from trade debtors. The turnover profile for the 40 companies with data is given by the green line in the graph below.




There are several factors that need to be considered in this data. Firstly, the £40m+ companies offer cyber security capability as one of many business activities, so it is not realistic to consider that their entire turnover is derived from cyber activity. In this case it is likely that the business units would operate as a medium sized enterprise, 50 to 250 people, with turnover at the higher end boosted by the global position of the larger enterprise £1M to £8M. Secondly, it is unlikely that this top end turnover would scale to the overall population, while there are 20% of companies in the sample it is

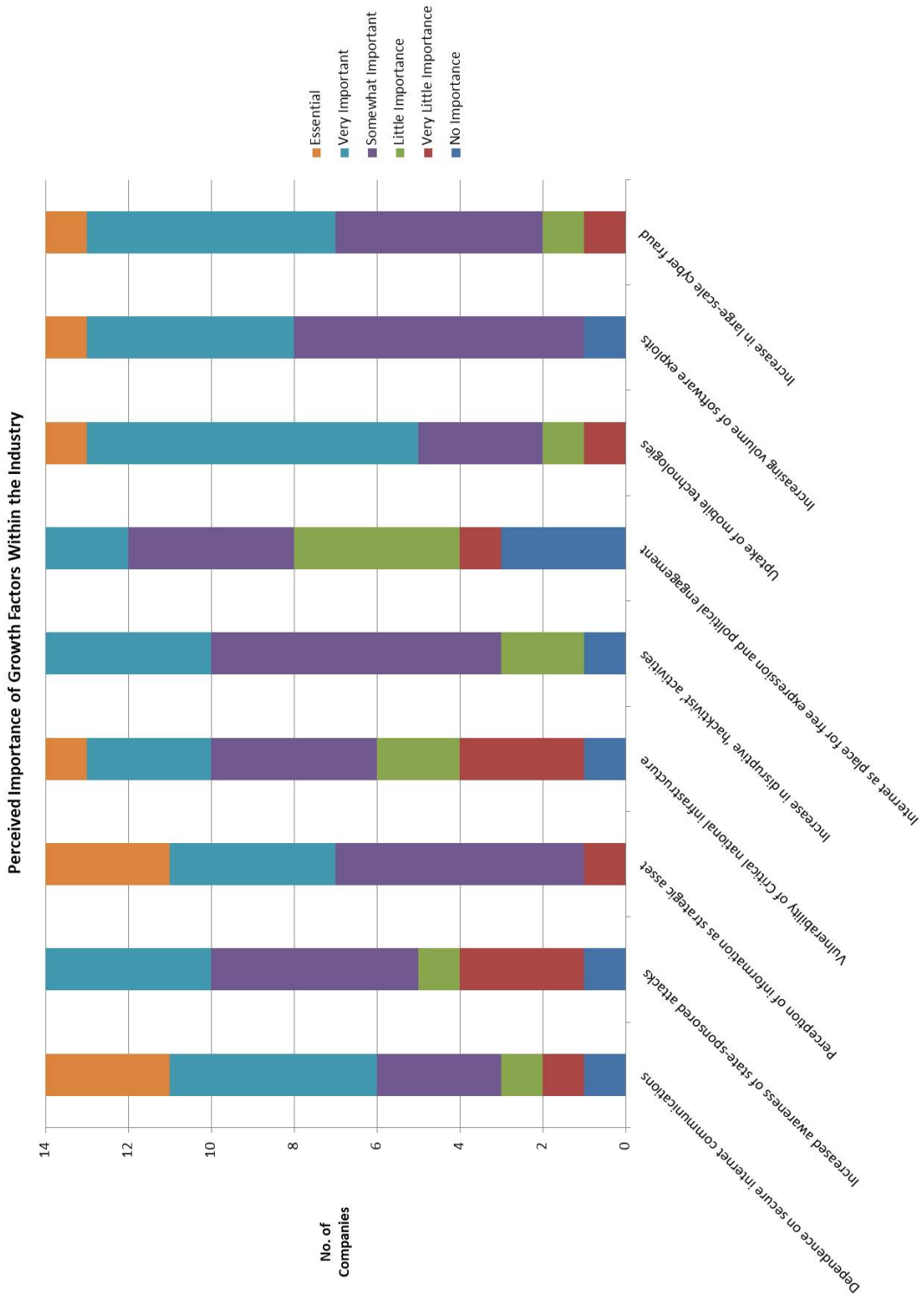
unlikely that there will be 20% in the total population (equivalent to 24 companies). Rather the lower end of the turnover profile is likely to be larger. Given these factors we can estimate the overall turnover of the cyber security industry by excluding the £40M+ outlier companies, inferring the remaining sample is representative of the larger population, then adding in the outlier companies and treating them as £1M to £8M turnover SMEs. In this case the estimated turnover in the North West is £355m per annum.

A further breakdown of the company size against company turnover is given below. It further illuminates the fact that the North West is made up of a large number of small companies operating in the £50k to £250k space. However, it is interesting to note that there is a peak still at the smaller end of employee head count that is generating high turnover levels in the £1m to £8m range. While this paints an interesting dynamic of those companies based in the North West, it is worth note that a large proportion of the company turn over data was estimated using trade debtors. The resolution of this approach is variable due to the economic climate potentially affecting the trade terms that suppliers offer.

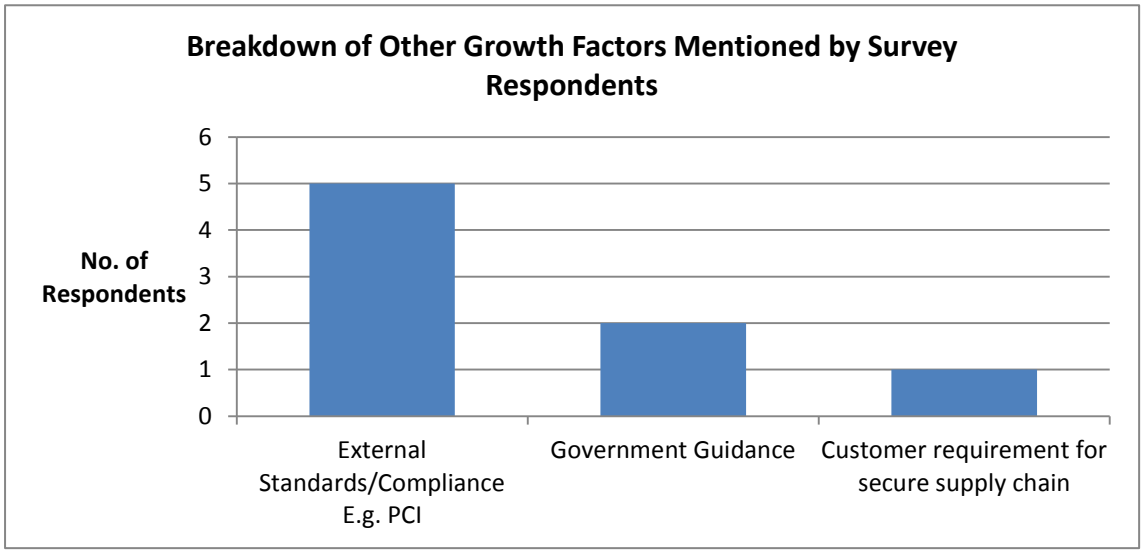



## Company Growth

The industry is clearly growing. The main drivers behind this growth are Perception of information as strategic asset and the Increasing volume of software exploits which threaten business. When asked to rate the factors which contributed to industry growth as part of the survey phase of this study respondents reacted overwhelmingly positively to information as a strategic asset and software exploits. The industry has developed because strategic decision makers understand the value of their business information and how fragile it is. However hacktivist activity does not concern the customers of the North West Cyber Security industry. Only 33.3% of respondents considered hacktivism to have a positive impact on industry growth.


Perceived Importance of Growth Factors Within the Industry
Essential
Very Important
Somewhat Important
Little Importance
Very Little Importance
No Importance
No. of Companies
0
2
4
6
8
10
12
14
Dependence on secure internet communications
Increased awareness of state-sponsored attacks
Perception of information as strategic asset
Vulnerability of Critical national infrastructure
Increase in disruptive 'hacktivist' activities
Internet as place for free expression and political engagement
Uptake of mobile technologies
Increasing volume of software exploits
Increase in large-scale cyber fraud

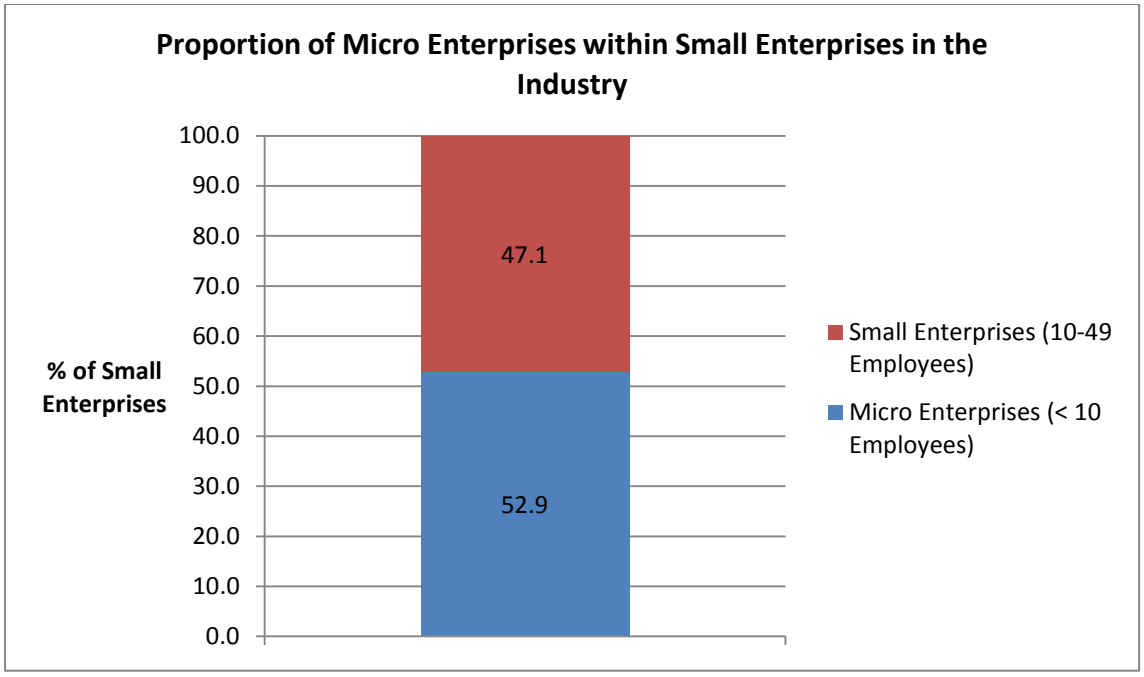
Three further driving factors were identified by survey respondents. The most important factor was External standards and compliance. The imposition of standards and the incentives to ensure compliance in data security were suggested independently by five respondents. Such standards include PCI DSO and ISO27001. Other suggested factors which were less popular included government guidance such as “The 10 Steps” and customers identifying the necessity of a secure supply chain.



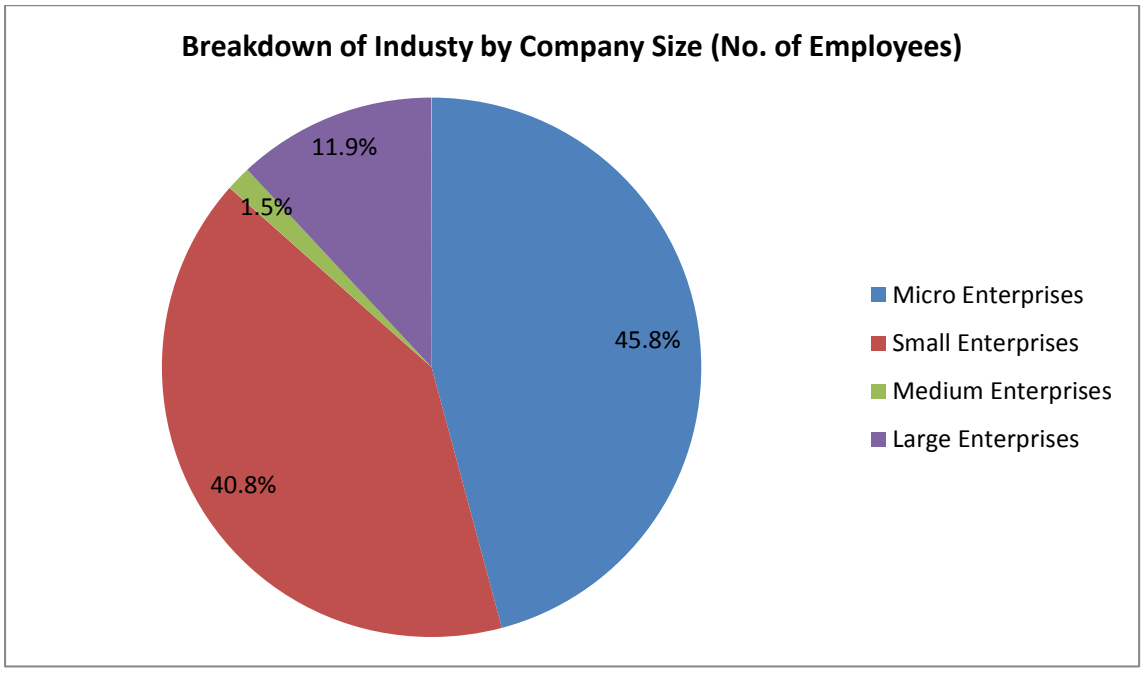

## Company Size (Employee Numbers)

Companies in The North West Cyber Security industry are overwhelmingly Small Enterprises. 87.3% of companies in The North West Cyber Security industry have fewer than 50 employees while 11.3% are classed as Large Enterprises with more than 250 Employees.

Confidence in this data is derived from the 59.1% of North West Cyber Security companies who we were able to get employee numbers information from. DueDil does not have a high enough resolution for companies with fewer than 50 employees to assess Micro Enterprises (companies with fewer than 10 employees). However our survey did account for micro enterprises. We found that 52.9% of those companies who replied to our survey had fewer than 10 employees.




Combining these statistics we can project that Micro Enterprises are the predominant company type in The North West Cyber Security industry.



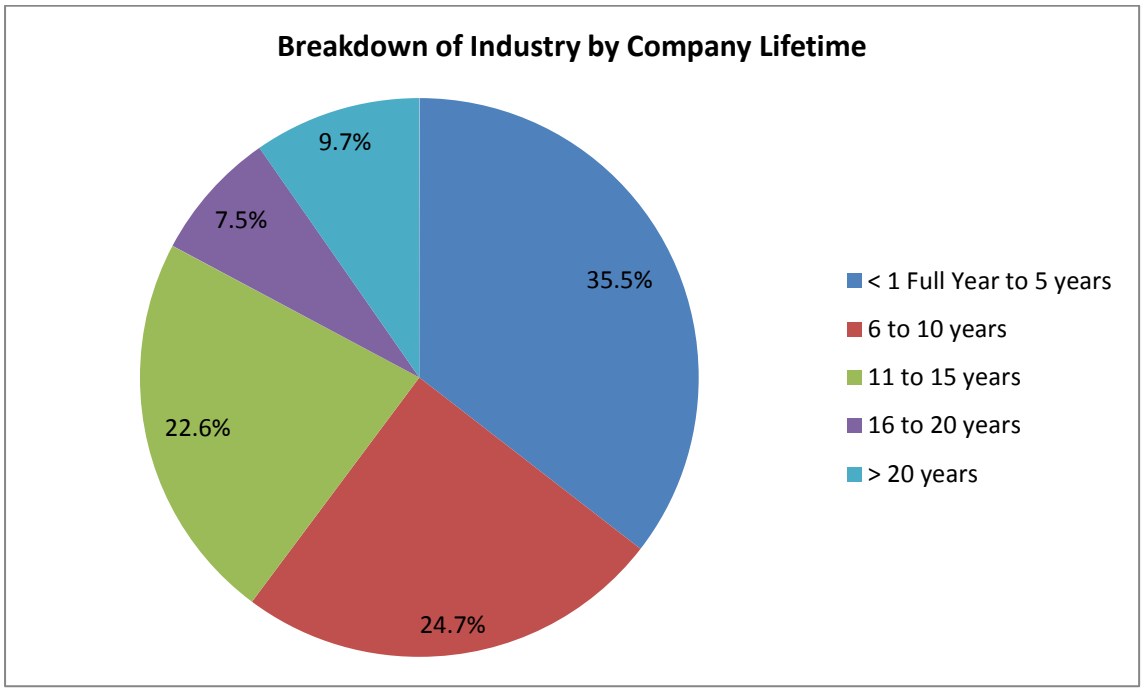

As with Turnover data we are seeing Medium Enterprises failing to take hold in the industry. In fact businesses with fewer than 50 employees make up the vast majority of the industry. As we will see this could be attributed to the relative youth of the industry. This makes the industry very dynamic and easily adaptable but may have an impact on the export capabilities of companies in the North West who are looking to export but do not have the operational capacity.

In 2014 the UK Private sector included 4.85 million Small and Micro Enterprises employing a total number of 11.35 million employees.[8] This suggests that the average Small and Micro Enterprise has 2.33 people on average. Along with a conservative estimate that all large businesses within the region have business units which consist of 50 people. It is possible conservatively project that the North West Cyber Security industry in 2014 employs more than 1,000 people.

## Company Lifetime

The North West Cyber Security Industry is fledgling. The mean age of a North West Cyber Security Company is close to 11 years. We were able to secure business establishment data from 93 companies (77.5% of the industry) therefore we can be confident about these figures. The 27 companies whose data was not taken into account were sole traders or partnerships for whom Companies House holds no data.

After dividing the companies into five year age groups we can see that the majority of companies within the North West Cyber Security Industry are less than five years old. 85.3% of the industry was established since 2000. This too may have an impact on the ability of the industry to export. An inexperienced staff with a developing UK customer base may be adverse to the perceived risk of entering overseas markets compared to an established force.




[8] Ward, Matthew & Rhodes, Chris. *Small Businesses and The UK Economy*. (December 2014). House of Commons Library Standard Note: SN/EP/6078. Available at: http://www.parliament.uk/briefing-papers/sn06078.pdf

# Conclusions

The North West Cyber Security Industry is young and growing.

The lack of clear SIC codes for cyber security businesses makes it a real task to identify cyber security businesses nationally. However it is clear that cyber security activities are not the preserve of a single kind of organisation, in fact cyber security has been capitalised on by a diverse set of organisations from technology driven start-ups to legal firms, insurance agencies and even large multinational business solutions providers such as KPMG and Deloitte. As a result supporting the cyber security industry will require engagement across sectors.

The industry is characterised by a split between Large and Small/Micro Enterprises. Small and Micro Enterprises constitute the vast majority of the industry. This generally low capacity of companies within the industry is borne out by turnover figures which saw the majority of businesses turning over less than £500,000 in 2014. Nevertheless 20% of the industry is currently turning over more than £40 Million and this minority is not only large multinationals who jumped on the cyber security bandwagon. There is genuine regional growth with players such as Daisy Group based in Nelson, Lancashire who turned over more than £350 Million last year.

It is concerning that there is such a limited Medium Enterprise sector within the industry. Only one (Avecto Ltd) of the 67 companies which supplied data to companies house had between 50 and 250 employees. This lack of Medium Enterprise may also explain the relatively tame proportion of the industry turning over between £1 million and £40 million. Research is needed to find out why there is such a divide in the North West.

Based on this demographic data it could be expected that few companies in the industry are in a position to export overseas based simply on generally low turnovers, small employee bases and few years to establish a regional or national customer base. It should be expect that large organisations in the upper reaches of both company size and turnover are the ones who are currently exporting. However the potentially high growth rates which are point to here demonstrate that the industry is growing strongly and so smaller operations have the potential to grow outside of the UK.

# Cyber Security Activities & Capabilities

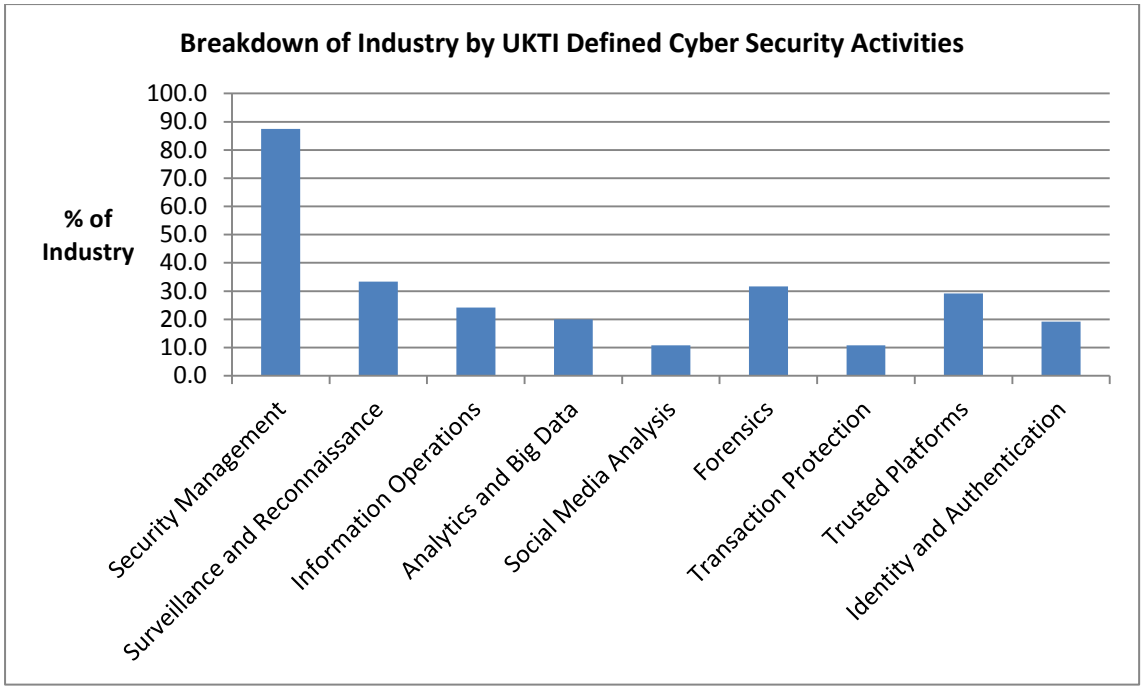
The most prevalent Cyber Security Activity in the North West Cyber Security Industry is Security Management. The majority of the industry is populated by a single SIC code (SIC 2007 62020) but there is a diversity amongst company classifications which suggests that many industries are diversifying into cyber security. Companies operate within their chosen activities in four many ways: Service Provision, Products, Integration and Design. Service provision is the most prevalent capability across all Cyber Security Activities however there is a significant portion of the industry which is guided by Design.

## UKTI Cyber Security Activities

The UKTI consider nine activities to fall under the umbra of cyber security. In the North West Security Management is by far the most prevalent activity undertaken by cyber security businesses. 87.5% of North West Cyber Security Companies perform Security Management activities. Security Management includes the operation, installation, design, reselling or integration of anti-malware software, data backup systems or other products/services which are used in the context of securing a customer's information or computer systems. Such activities can include real-time crisis management systems or policy planning for data security. Security Management is sold either as a onetime item (e.g. installation or integration of systems) or as part of a service contract for ongoing service provision. The popularity of Security Management may be driven by a combination of the industry growth factors discussed in the previous section but in particular by External Standards such as PCI DSS and ISO 27001.

Transaction Protection and Social Media Analysis were the least well subscribed activities in the North West Cyber Security Industry with only 10.8% of companies taking part in either activity. Transaction Protection includes products or services which allow for secure transactions of information from end-to-end in environments with variable trust levels. Social Media Analysis includes the capture and analysis of social network activity, to establish digital profiles, understand influence, monitor trends and observer sentiment. There may be barriers to operation in these activities, in the case of transaction protection there are established global businesses such as Paypal and Visa. In Social Media Analysis privacy and data protection laws may form a barrier to entry.

There are businesses operating in all nine of the UKTI Cyber Security Activities in the North West. This study identified at least 13 businesses operating in each of the UKTI's nine activity areas. While there is a clear distinction between Security Management and the less subscribed to activities, those niche activities are still present in the region. This is encouraging because it suggests that the North West has technical expertise across cyber security activities.



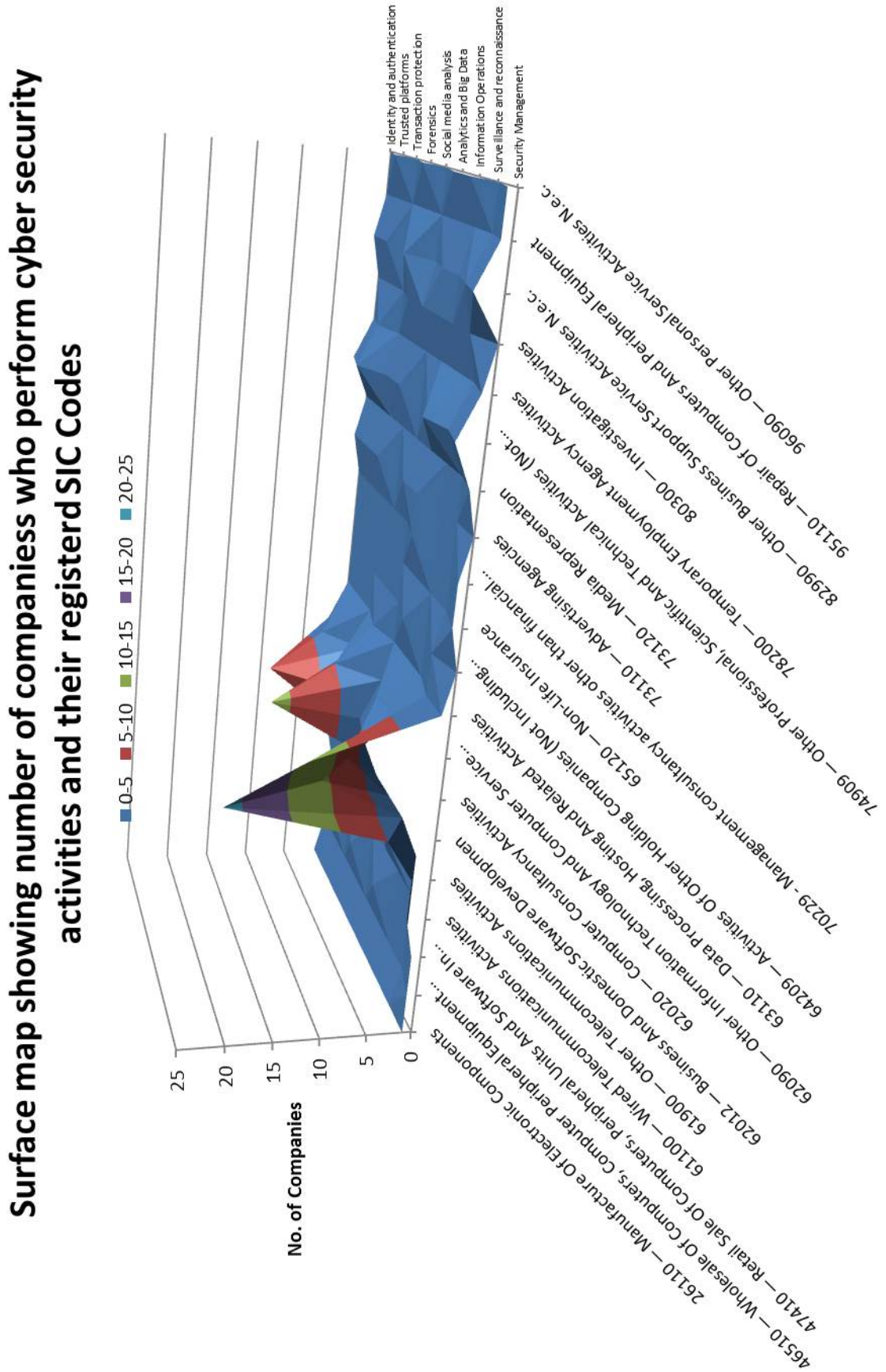

## Activities cross referenced with SIC Codes

While there is no specific SIC code to describe Cyber Security businesses the SIC 2007 code "62020 – Computer Consultancy Activities" is by far the most significant within the North West Cyber security industry. 39.7% of cyber security businesses in the North West with SIC 2007 codes are registered under 62020.

The graph below represents the 73 companies identified in the study who have a registered SIC 2007 code. It shows the number of businesses who take part in each UKTI cyber security activity within each SIC code. This visualisation reveals that there are five or fewer businesses operate in each activity that are registered under each of the identified 20 SIC 2007 codes. Computer Consultancy Activities is the clear exception to this uniformity with elevation across activities and three spikes representing a large population of Security Management, Forensics and Trusted Platforms companies.

The sloping sides of these spikes reveal SIC codes which support Computer Consultancy Activities. Other significant sic codes include "62012 — Business And Domestic Software Development" which has a significant Security Management element (five businesses) and "62090 — Other Information Technology And Computer Service Activities" which has significant Security management and Surveillance elements (14 and seven businesses respectively).

This SIC code analysis demonstrates that there is a diversity within the North West Cyber Security Industry. While the core of the industry is registered as computer, technology or software development companies there are 20 classifications of company who are active within cyber security. This suggests that companies are diversifying into cyber security from disparate industries.

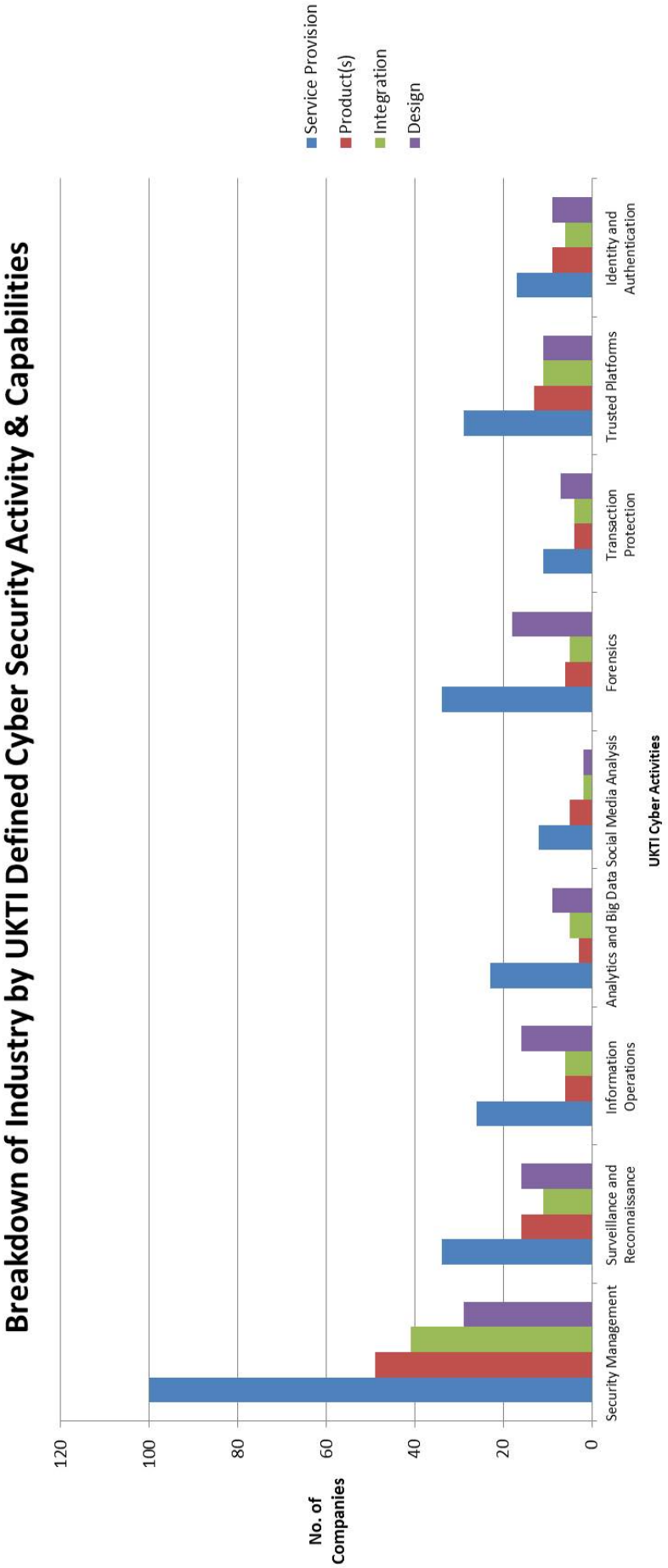

Surface map showing number of companiess who perform cyber security activities and their registerd SIC Codes
0-5
5-10
10-15
15-20
20-25
No. of Companies
0
5
10
15
20
25
Identity and authentication
Trusted platforms
Transaction protection
Forensics
Social media analysis
Analytics and Big Data
Information Operations
Surveillance and reconnaissance
Security Management
46510 — Wholesale Of Computers, Computer Peripheral Units And Software In...
26110 — Manufacture Of Electronic Components
47410 — Retail Sale Of Computers, Peripheral Units And Software In Specialised...
61100 — Wired Telecommunications Activities
62090 — Other Information Technology And Computer Service Activities
61900 — Other Telecommunications Activities
62012 — Business And Domestic Software Development Activities
62020 — Computer Consultancy Activities
63110 — Data Processing, Hosting And Related Activities
64209 — Activities Of Other Holding Companies (Not Including...
70229 - Management Consultancy Activities Other Than Financial...
65120 — Non-Life Insurance
73110 — Advertising Agencies
74909 — Other Professional, Scientific And Technical Activities (Not...
73120 — Media Representation
78200 — Temporary Employment Agency Activities
82990 — Other Business Support Service Activities N.e.c.
80300 — Investigation Activities
95110 — Repair Of Computers And Peripheral Equipment
96090 — Other Personal Service Activities N.e.c.

# Activities and Capabilities

By assessing how companies operationalise the UKTI Cyber Security Activities it is possible to gain deeper insight about the nature of the North West Cyber Security Industry. Four capabilities were identified which apply to cyber security businesses: Service Provision, Products, Integration and Design (See Appendix 2 for more information).

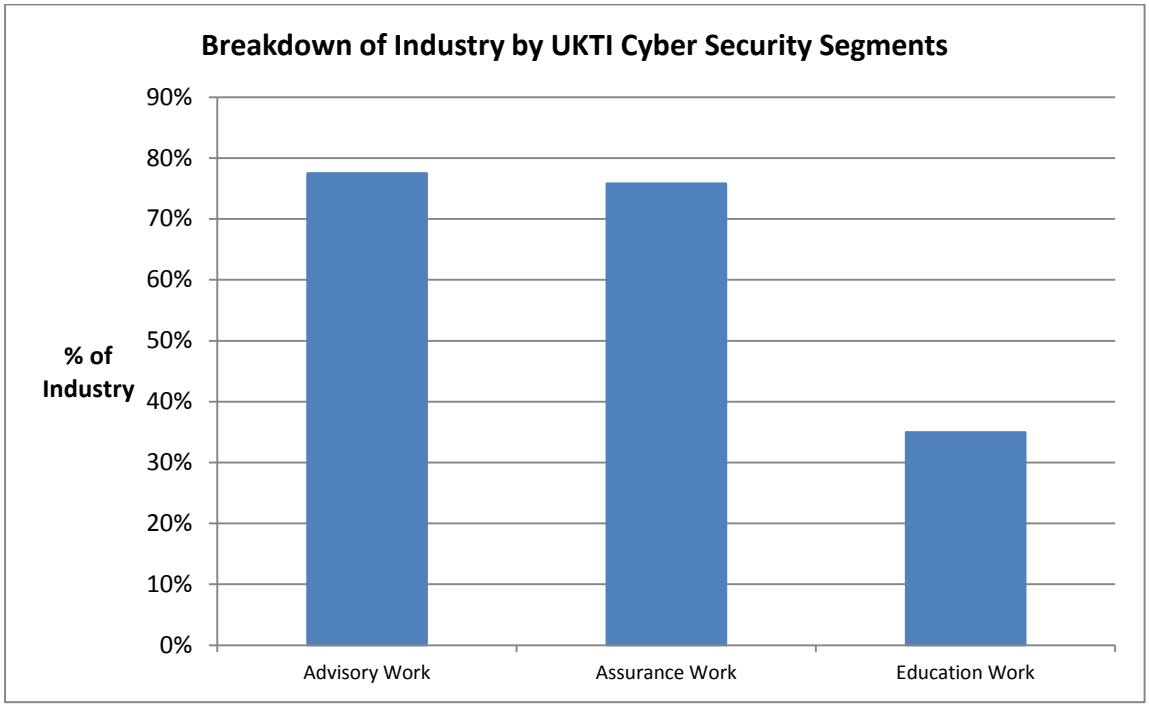
Service Provision is uniformly the most significant capability across activities carried out in the North West Cyber Security industry. More companies have the capacity to provide services than products, integration or design in each of the UKTI cyber security activities. In the case of Security Management 83.3% of the north west cyber security industry provide service provision whereas 40.8% of companies provide Products for resale (the second largest capability in Security Management). This demonstrates that service provision is an extremely attractive capability for cyber security companies. In particular Service Provision in Security Management is attractive. One reason that Service Provision may be more appealing to the industry than other activities is the earning potential of ongoing Service Provision agreements.

Encouragingly Design is a relatively prevalent capability amongst those companies who take part in Surveillance and Reconnaissance, Information Operations, Analytics and Big Data Analysis, Forensics, Transaction Protection and Identity and Authentication. In each of these instances Design was the second most prevalent capacity behind Service Provision. This demonstrates that innovation is a more significant driver in the North West Cyber Security Industry than integration of existing products and reselling of existing products.


Breakdown of Industry by UKTI Defined Cyber Security Activity & Capabilities
Service Provision
Product(s)
Integration
Design
No. of Companies
0
20
40
60
80
100
120
Security Management
Surveillance and Reconnaissance
Information Operations
Analytics and Big Data
Social Media Analysis
Forensics
Transaction Protection
Trusted Platforms
Identity and Authentication
UKTI Cyber Activities

# UKTI Segmentation

In addition to the UKTI Cyber Security Activities the UKTI identifies three Segments in which cyber security companies can be located. The majority of the North West Cyber Security industry takes part in Advisory (77.5%) and Assurance (75.8%) work however only 35% of the industry takes part in Educational work. There are a number of potential reasons for this based on the demographic data detailed earlier. Educating external organisations is time and resource intensive and requires a great deal of experience. 87.5% of the industry is classed as a Small or Micro Enterprise. 60% of the industry turned over less than £1 Million in 2014. 59.1% of businesses are less than a decade old. It is therefore unsurprising that the more profitable core business operations of advice and assurance are more prevalent than education.




# Conclusion

This data creates a picture of the North West Cyber Security Industry which has a significant focus on Security Management most likely due to the demand for this activity in the form of Service Provision. This business model is attractive because it involves long term service contracts. However the industry is also diverse and innovative with a large number of companies who have a capacity to design new products. There are companies who operate in every capacity across all nine activities which further demonstrate that the industries diversity. The weakest activities in the industry include Social Media Analysis and Transaction Protection however there is innovation in the form of design capabilities in each of these activities.

Detailed SIC Code analysis demonstrates that the 62020 SIC 2007 code is the most common amongst all of the Cyber Security Activates. Furthermore there is interest across the activities in up to 19 different company classifications. This suggests that non-computing businesses are diversifying into cyber security. As a result it is important for any intervention in the industry to nurture the core of computing businesses and those businesses who seek out opportunities in a new area.

North West Cyber Security businesses are less inclined to take part in education work than advisory or assurance work. This is likely to be due to demographic profile of many of the majority of the industry. More research is needed in order to understand if education is demanded in the region or if there is a role for government in this area. A strong understanding of cyber security in the region would likely lead to industry growth.

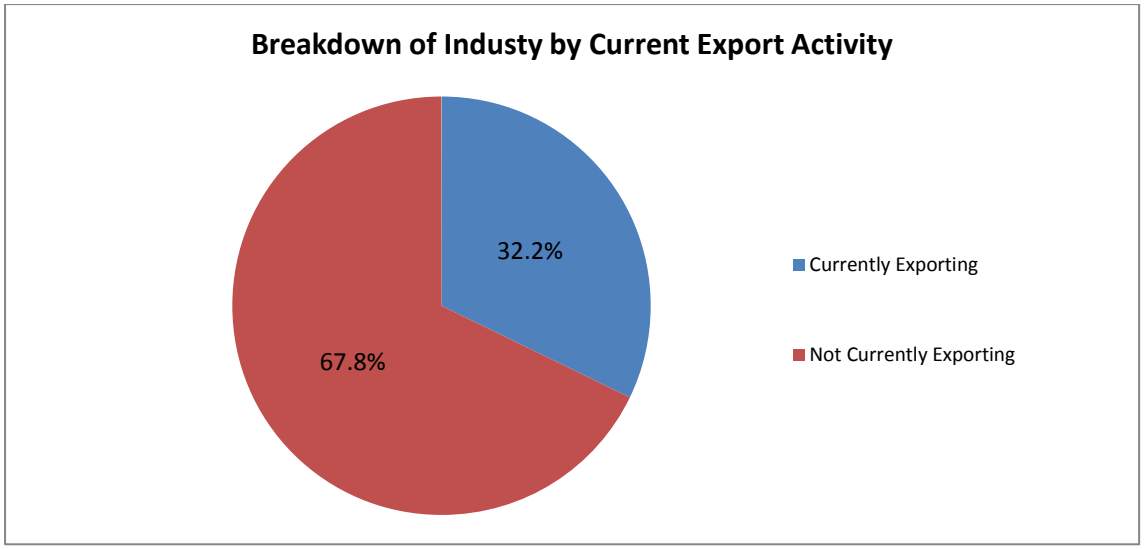
# Export Activity and Potential

A significant portion of the North West Cyber Security Industry is currently exporting products and services overseas. Export destinations range and include global players and those who are restricted to Europe or other English speaking countries. The UKTI's Priority Markets are not currently being addressed by the North West Cyber Security Industry, instead the region is focused mainly on expansion in Europe. There is limited interest in the kinds of overseas projects which the UKTI hopes to encourage. Companies are to some extent confident of their ability to operate overseas but it is clear that they are not currently following the UKTI Export Strategy.

While the data collected is as rigorous as possible, the reader should note that the sample size regarding export data is much smaller than the overall population. Thus far the report has shown that the direct questioning survey data is representative of the overall population demographic data (see page 11) giving the research team confidence in extrapolating the sample data to the wider population.

## Current Exports

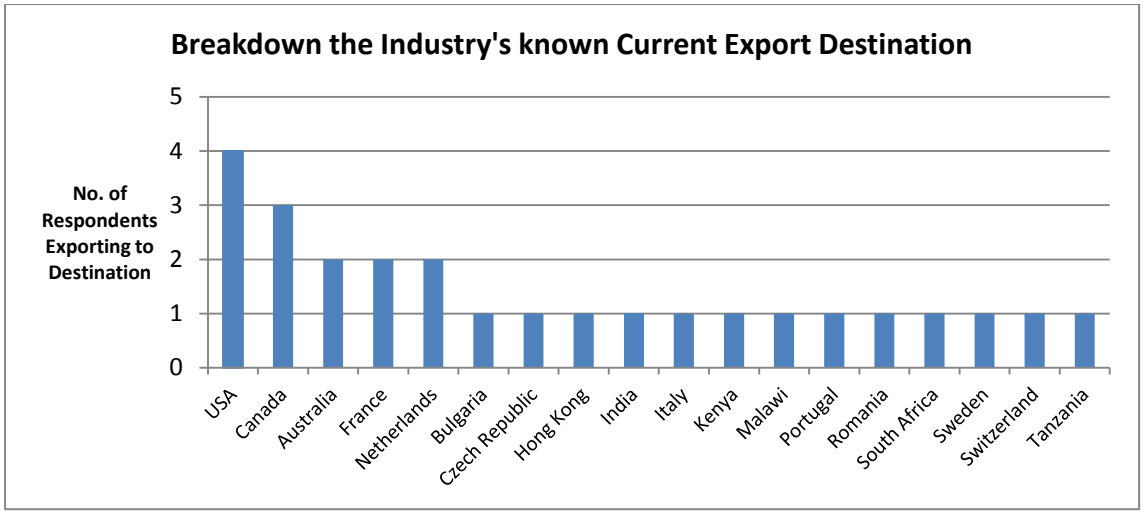
Based on the research data, it is estimated that around one third of businesses in the North West Cyber Security Industry currently export their goods or services. From the directly surveyed companies 13 out of 27 respondents (48%) indicated they currently exported. Including the data obtained from the website analysis it is shown that 19 out of 59 (32%) companies are certain to be exporting while 30 companies are certain are not, leaving 61 companies with no detailed information. It has been shown that the collected data is representative of the overall population, through demographic analysis for example implying the remaining 61 companies have a similar profile to those in the sample set. In this case, 32% of the total population is exporting giving around 38 companies in total. Beyond this we can also define the firm upper and lower bound values for the number of companies that are exporting. The data shows that 19 companies are exporting with 30 companies definitely not. Therefore, at a minimum 16% of the companies are exporting and at a maximum 75% are. This provides further confidence in the expected figure of 32% (at the lower end of this range) companies exporting. A current export rate of between 32% is highly encouraging, demonstrating demand from overseas and a willingness in the North West to supply.




## Known Destinations

English speaking nations and Europe are the most popular export destinations amongst businesses in the North West Cyber Security Industry. Survey respondents were asked to list the countries they exported to. The USA and Canada were identified to be the most popular destination while eight European countries and four African countries were mentioned by name. Hong Kong and India were mentioned once each, they are the only Asian countries to be mentioned by survey respondents. This list of 18 export destinations presented here is not entirely representative of the industry. 10 respondents failed to list their export destinations as they classed their operations as global. This data demonstrates that there is a diversity amongst export destinations. Furthermore the industry has a mixture of very specific exporters working with one of a few other nations and global operators.

Of those respondents who listed specific destinations it is notable that there was no mention of Russia, China or South America. Of the UKTI Priority Markets as established by the UK export strategy only India was present. There are clear political or linguistic reasons for not exporting to these destinations none of which are English speaking furthermore many of the UKTI priority markets are situated in the volatile Middle East. Fears over language barrier were identified anecdotally via survey responses, political fears were not.




# Export Potential

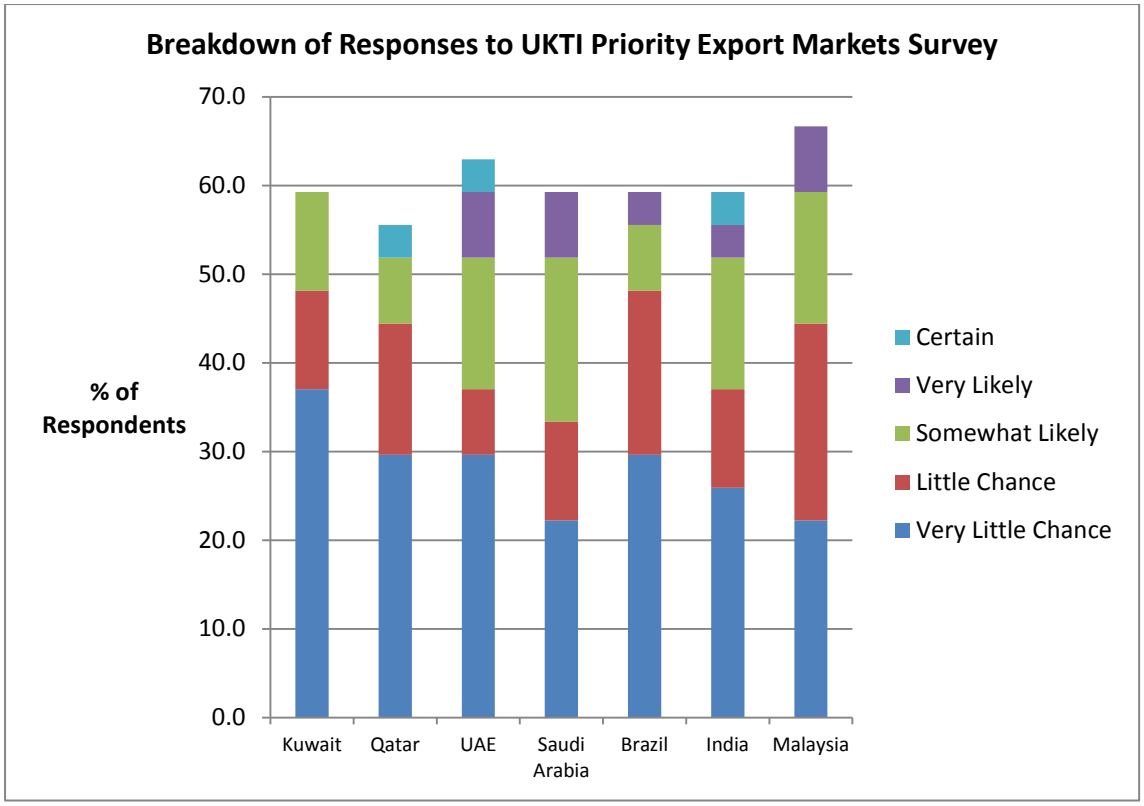
Some businesses in the North West have no interest in exporting their cyber security products or services. 21.7% of companies surveyed demonstrated that they were interested in providing services for their local area only. As previously noted the Micro/Small Enterprise nature of the industry may explain this. Resource and operational capacities simply might not exist for many of their businesses. It is also possible that many of these businesses do not recognise that they have exportable services, a large number of these companies are local PC repair shops or Sole Traders who dabble in back up service and ant-virus software.

## UKTI Priority Markets

The North West Cyber Security Industry is interested in some of the UKTI's Priority Markets. Qatar, UAE and India all had one or more "Certain" responses form surveyed businesses.

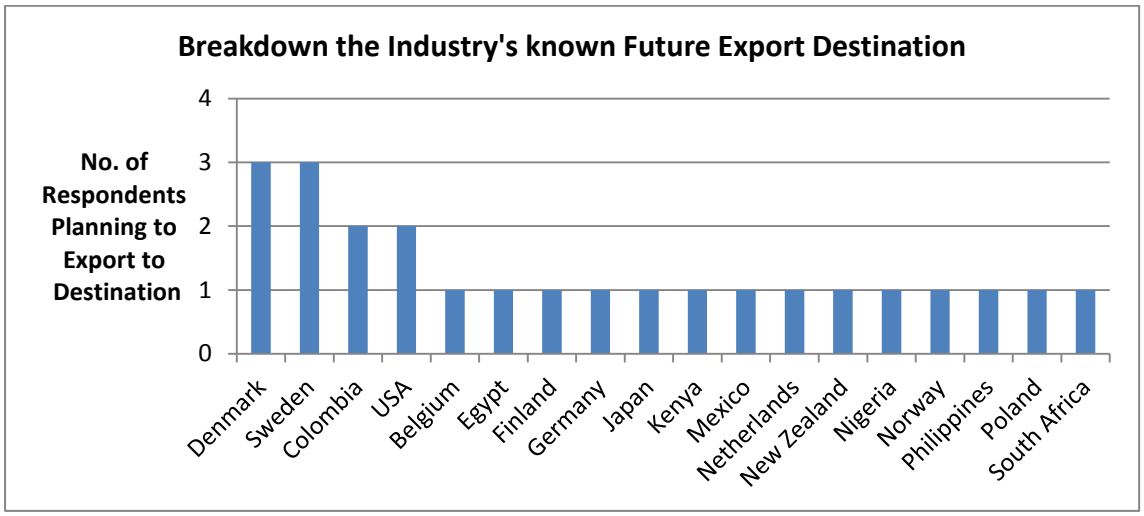
However 29.6% of respondents explained that they had "No Chance" of exporting to any of the UKTI Priority Markets. Some had no interest in exporting at all, some were focusing on other export destinations.

The most positively received suggestions were Saudi Arabia and UAE. 25.9% of respondents suggested there was a degree of likelihood (between "Somewhat Likely" and "Certain") that they would export to either Saudi Arabia or UAE. This may be because of knowledge of existing business relationships between these nations and the UK, particularly in the areas of security and defence.



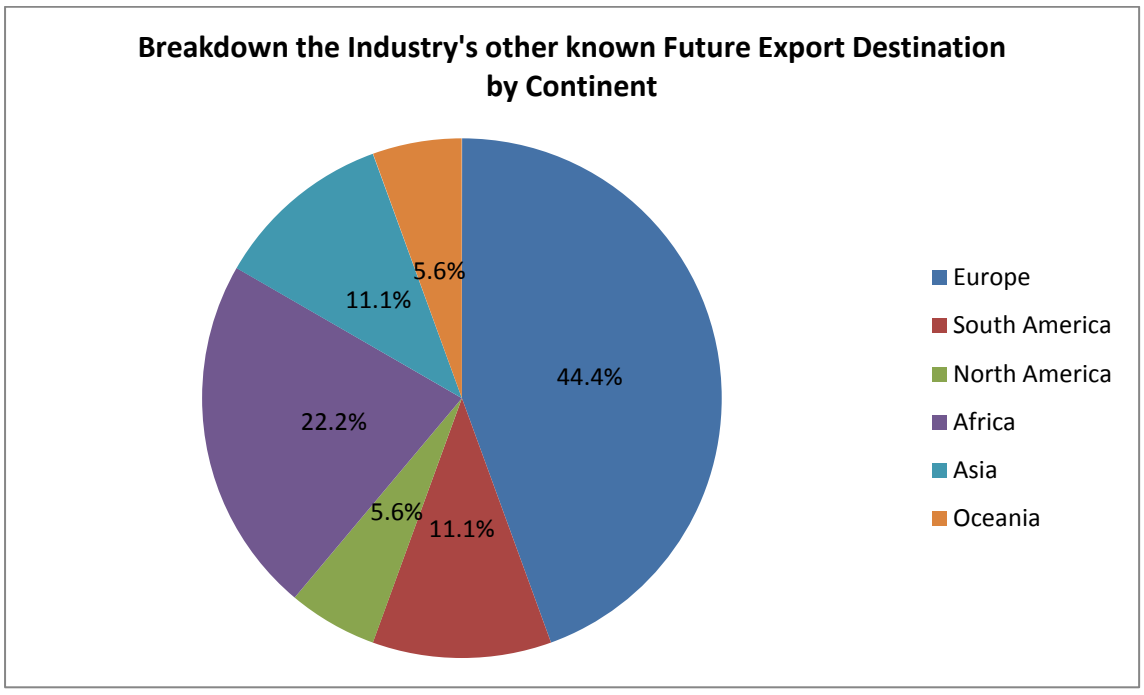

## Other Future Markets

While there was interest in UKTI Priority Markets it appears that the industry is focused on alternative export destinations. Denmark and Sweden were the most popular destinations mentioned by respondents. This is especially interesting considering that the language barriers which exist in both of these countries. English speaking countries account for only three of the 18 countries mentioned by respondents.




18 individual countries were identified in by respondents. The majority of planned export expansion will take place in Europe 44.4% of export destinations were European. This is unsurprising considering the incentives for trade within the EU such as proximity and lack of tariffs.

There is further interest in Africa, Asia and South America. Once again China and Russia were not mentioned as planned export destinations. There are clearly few incentives to work with two of the largest economies on Cyber Security projects.

# Potential Export Products/Services

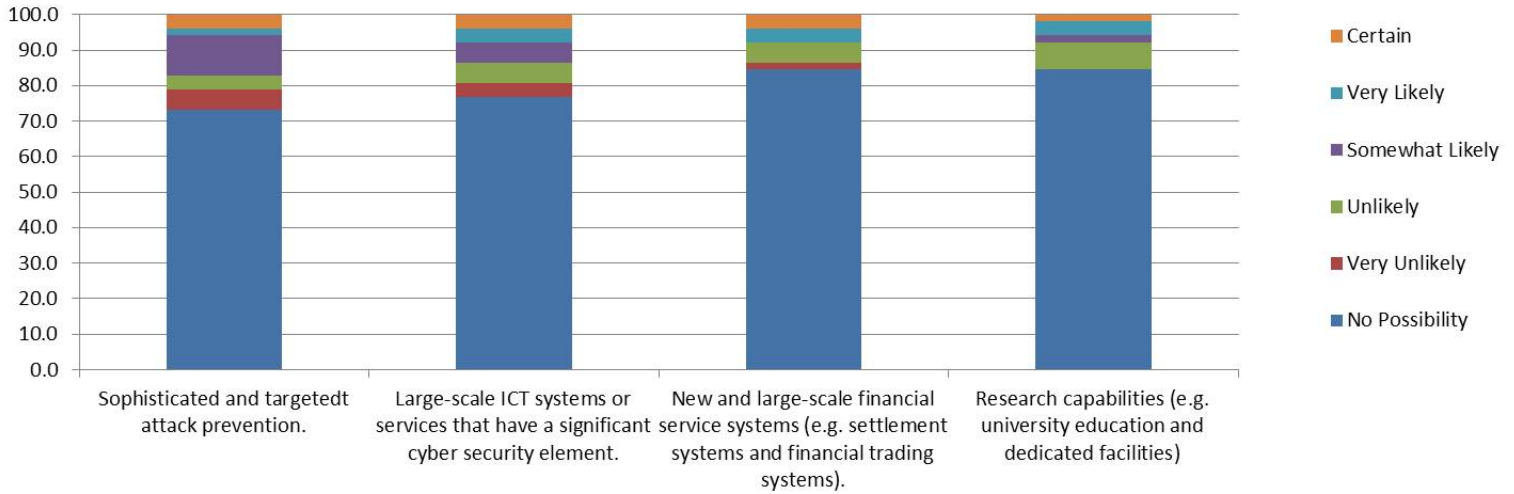
In addition to specific export destinations survey respondents were asked to rate the likelihood of their business exporting specific products and services outside of the UK. The four products or services discussed were:

- Sophisticated and targeted attack prevention
- Large scale ICT systems or services that have a significant cyber security element
- New and large scale financial services systems
- Research capabilities

The most popular of these export options was Sophisticated and targeted attack prevention with 17.3% of respondents considering it “somewhat likely”, “very likely” or “certain” that they would export such products or services in the future. The least positive response came for financial systems and Research capabilities with 7.7% of respondents having positive feelings towards each of these paths. These low figures are to be expected considering the capacity required to carry out large scale operations in another country and the demography of the average North West Cyber Security company.

However there is evidence that North West businesses will be working in even the most complex ventures overseas. 3.8% of businesses were certain to be taking part in attack prevention, large scale IT services and large scale financial service systems in the future. Elements of the industry clearly have the capacity to deal with highly complex challenges outside the UK.

**Breakdown of Attitudes of Respondents to Export Products/Services Survey**



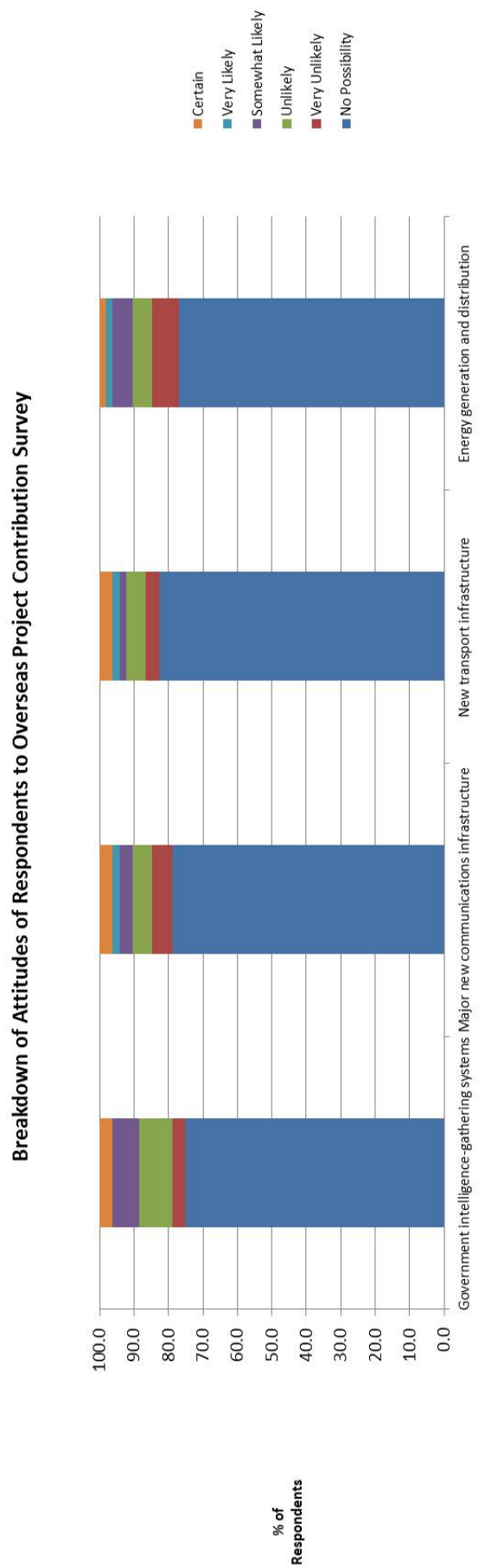
## Potential Overseas Projects

A similar story is apparent when companies were asked about the potential to collaborate on projects overseas. There was a generally poor interest in such activities, more than 75% of respondents rejected the possibility to collaborate on each of the potential project types. The project types suggested were:

- Government intelligence-gathering systems
- Major new communications infrastructure
- New transport infrastructure
- Energy generation and distribution

Government intelligence gathering systems were the best received by companies. 11.5% of companies responded positively about the likelihood of their involvement in overseas operations in the field of intelligence gathering systems in the future. New transport infrastructure was the least well received with only 7.7% of those surveyed responding positively.

Elements of the industry will be collaborating on all of the suggested projects. 3.8% of companies were certain that they would carry out such work overseas in the future, apart from in the case of energy generation where the rate of “certain” companies was smaller (1.9%)

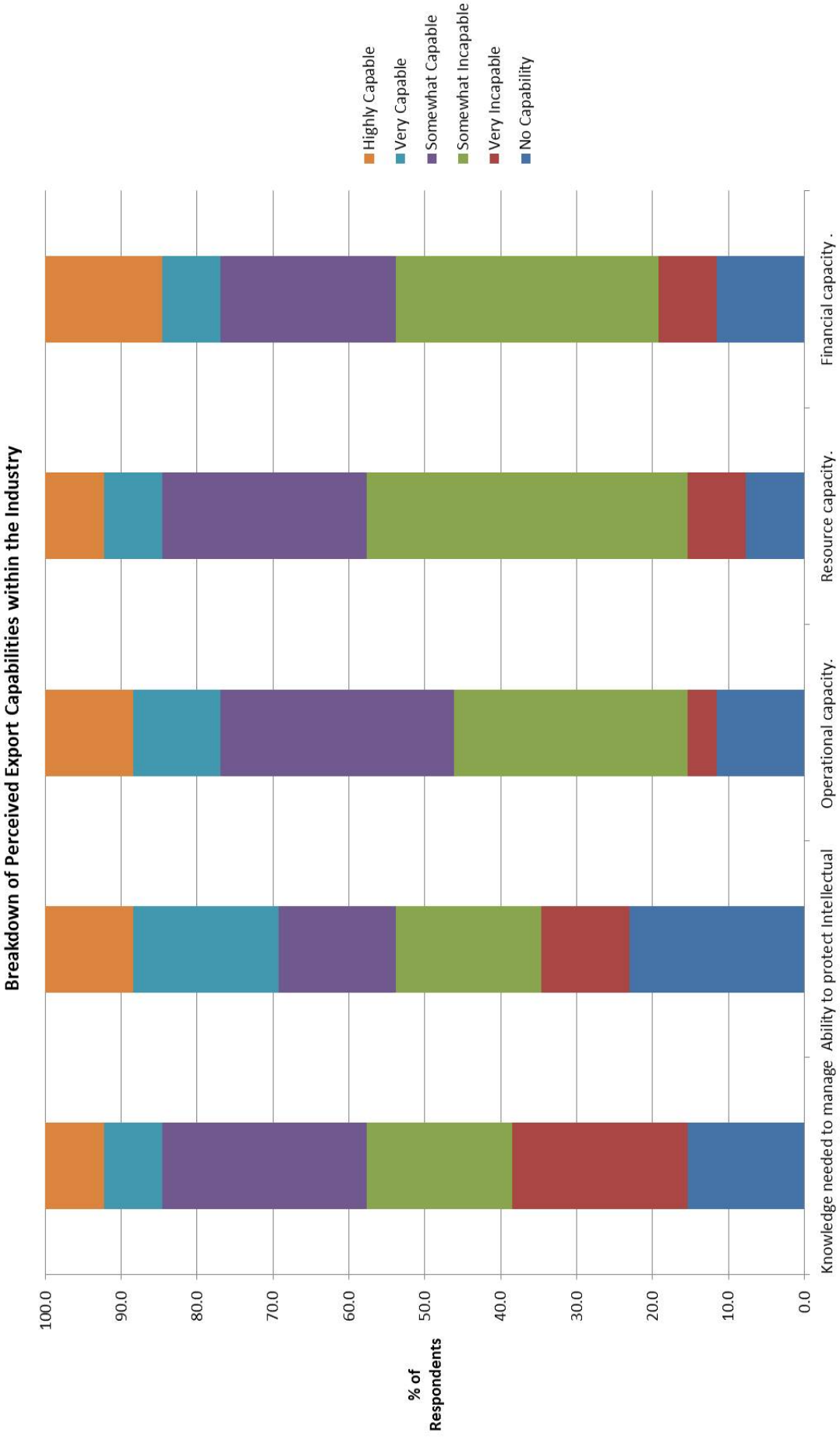

Breakdown of Attitudes of Respondents to Overseas Project Contribution Survey
% of Respondents
100.0
90.0
80.0
70.0
60.0
50.0
40.0
30.0
20.0
10.0
0.0
Government intelligence-gathering systems
Major new communications infrastructure
New transport infrastructure
Energy generation and distribution
Certain
Very Likely
Somewhat Likely
Unlikely
Very Unlikely
No Possibility

## Perceived Export Capabilities

In order to get a better idea about the reasoning behind the export likelihood responses the study asked respondents to rate their export capabilities. As a result perceived capabilities within the region can be discussed. Five key capabilities were discussed:

- Knowledge needed to manage an overseas market entry
- Ability to protect Intellectual property overseas
- Operational capacity
- Resource capacity
- Financial capacity

Most of the industry considers itself to have the operation capacity to carry out exports. 53.8% of respondents replied positively when they considered how they felt about their company's operational capacity. However fewer respondents were confident about resource capacity or their knowledge of overseas markets. While most businesses see their staff as having the capability to manage business overseas they are concerned by their lack of local and linguistic knowledge.


Breakdown of Perceived Export Capabilities within the Industry
Highly Capable
Very Capable
Somewhat Capable
Somewhat Incapable
Very Incapable
No Capability
% of Respondents
100.0
90.0
80.0
70.0
60.0
50.0
40.0
30.0
20.0
10.0
0.0
Knowledge needed to manage an overseas market entry.
Ability to protect Intellectual Property overseas.
Operational capacity.
Resource capacity.
Financial capacity .

# Conclusion

There is a clear discord between the UKTI Export Strategy and what is currently taking place in the North West Cyber Security industry. Only a small percentage of the industry is interested in exporting to the UKTI's priority markets. A trend that is carried on when questioned about the overseas activity and collaborations which companies might be involved in in the future. Some of this can be explained by portion of the industry who operate on a local basis as PC repair shops or local business support providers, businesses who been identified to have no intention of exporting.

However the study has identified that 32%-48% of companies in the North West are already exporting, 12% of the industry is exporting globally. The survey portion of this study identified 19 individual countries which the industry would be moving into in the future. Surveying perception of export capacity the picture is mixed but there is a clear section of the industry that feels highly capable.

This disconnect suggests that the UKTI may have to incentivize the North West Cyber Security Industry to follow its export strategy . Requirement for Language and local knowledge support was a recurrent theme interviews with business owners. In addition there was anecdotal evidence that elements of the industry are beginning to look at South America as a future market due to a perceived lack of knowledge and economic growth in the region. This is assertion is corroborated by the data collected. There is currently no evidence of exports to South America and yet 11.1% of the industry plans to export there in the future.

# Collaboration

The majority of businesses in the industry have not engaged with government departments. The engaging department has been The Home Office with mixed success. GCHQ and the UKTI DSO are the most popular amongst those who have engaged with government departments. Unsurprisingly the North West Cyber Security Industry collaborates with Government, Business and Academia in the UK more than they do overseas. However there is a clear capability to work with overseas partners, this discovery reinforces the perception of export capabilities by the industry in the previous section.

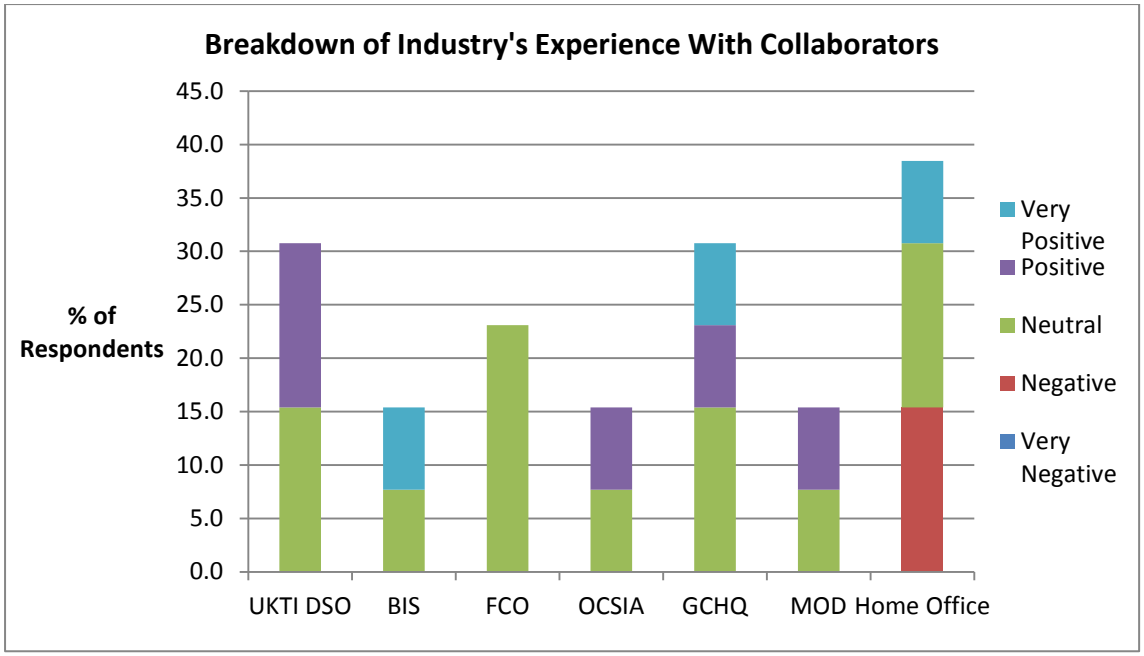
## Collaboration Experience

### UK Government Department Engagement

The only department to have received any negative feedback in this study regarding collaboration is The Home Office. 15% of respondents felt negativity as a result of their dealings with the Home Office. However The Home Office has some very positive feedback. It seems that interactions with the Home Office have been polarising.

This is not the story throughout collaboration with other departments. In general there is a feeling of neutrality to interactions with government departments with some positivity. The most positive interactions have been with UKTI DSO and GCHQ. 15.4% of respondents considered their interactions with these departments to have been either “positive” or “very positive”. Considering the nature of the work of GCHQ when compared to the other departments suggested this is understandable. GCHQ work in the field of cyber security here The Home Office or FCO (for example) do not. It is good to see a generally positive outcome for UKTI DSO. It is encouraging that the industry is receptive to the UKTI’s work.

The big story in this data is that very few respondents had ever had interactions with government departments. Indeed The Home Office was the most engaged with department and yet 61.5% of respondents had not worked with The Home Office. BIS, OCSIA and MOD were the least engaged with each having 84.6% of respondents reply “No Engagement”. This may meant that (for better or worse) The Home Office has a more effective outreach strategy with the industry. However interviews with business owners suggest that engagement directly with departments is not necessarily desired some saw it as unprofitable and a waste of time and some could not see the value in engaging with government.



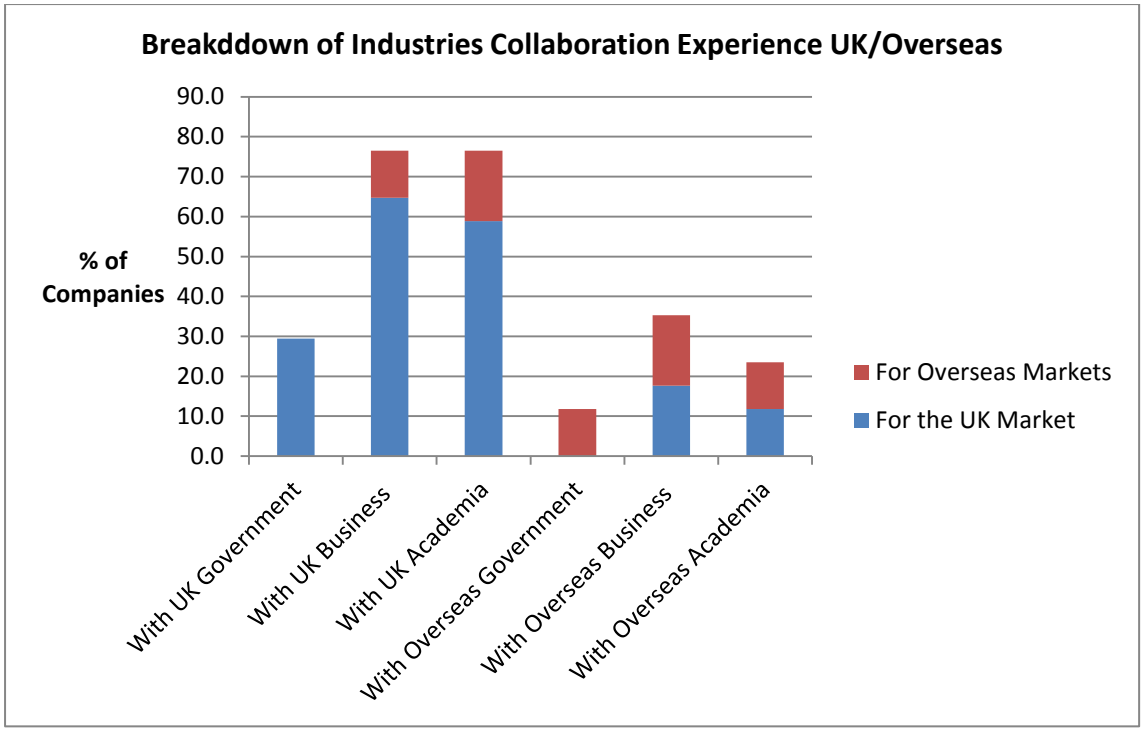

## Collaboration Experience UK/Overseas

It was deemed important to understand how companies within the North West Cyber Security Industry interacted with Government, Business and Academia both inside the UK and Overseas. In addition the study sought to find which market (UK or Overseas) would benefit from these collaborations.

Collaborations within the UK for the UK market were the most popular amongst respondents. 64.7% of respondents had collaborated with other UK businesses on projects within the UK market and 58.8% of respondents had collaborated with UK Academia for the UK market. This demonstrates that the industry is happy to work alongside other businesses and more unusually that the industry is capable of working with academia. This is likely to be a perk of the knowledge based nature of the cyber security industry as a whole.

Collaboration with government was low. This may be expected looking at Engagement with Government Departments presented earlier. Only 29.4% of respondents had collaborated with the UK Government and all of those collaborations were for the UK market. 11.8% had collaborated with overseas governments. Unsurprisingly those collaborations were for the overseas rather than UK market. Any dealings with overseas governments which affect the UK market would most likely entail engagement with the UK government also. This is a clear growth area for the industry.

Collaboration with Overseas business and academia is much more limited collaboration with partners based in the UK. However there is evidence of North West Cyber Security Companies collaborating with both business and academia overseas. 17.6% and 11.8% of respondents had worked with overseas business and academia respectively on projects targeted at overseas markets. This suggests that the confidence expressed in respondents perceived export capabilities is indeed accurate, parts of the industry does have the capacity to export successfully.




# Conclusion

Interactions with the UK government have been limited to UK projects. Engagement with The Home Office has led to mixed feelings in the industry but collaboration with GCHQ and UKTI DSO has been more positive. 38.5% of respondents have never engaged with the UK government departments discussed. There may be greater scope for GCHQ to interact within the industry. They have been given positive feedback and there should be synergy between the department and the knowledge based operations of the industry. It should be noted that some of those individuals who were contacted via telephone remarked that they had no desire to engage with government as they saw such interactions as time consuming and unprofitable.

Collaboration on projects is clearly something which the industry is capable and comfortable doing. Indeed the nature of complex it systems requires synergy between businesses. Only 7.7% of respondents had not collaborated with Government, Business or Academia either inside or outside the UK. The creation of partnerships and collaborative projects is something that the industry may welcome.

# Case Studies

## The Computer Doctor Liverpool

Does not export. Does not want to export.

The Computer Doctor Liverpool is a home and small business IT Support Company supplying the Liverpool area. The Computer Doctor Liverpool focuses on supplying a timely and high quality service of comprehensive IT systems support to individuals and small business including hardware and software support, hosting and cyber security measures. Support and advice can be acquired from The Computer Doctor Liverpool in a one off instance or as part of a monthly support contract.

Open Source Data about The Computer Doctor Liverpool was gathered from their website. The company is run as a Sole Trader and so financial information was not available. The company was contacted as part of the survey process and the business owner was interviewed.

### Cyber Security Activities/Capabilities

The Computer Doctor Liverpool has been categorised as a cyber-security company falling under the Cyber Security Activity Security Management. They are capable of service provision and reselling products. They perform cyber security advisory and assurance work but they do not provide education and training.

Specific Security Management services advertised on The Computer Doctor Liverpool's website include "Online Backup Services", "Data Recovery" and "Virus cleansing".

### Export Activity & Export Readiness

The Computer Doctor Liverpool does not currently export its products or services outside of the UK nor does the company owner intend to expand into overseas markets anytime in the future. This includes into the UKTI priority markets.

When asked to rate the companies capacity to enter overseas markets it becomes clear why the owner does not wish to, or is unable to, enter overseas markets.

| The respondent was asked to rate each capacity from 1-6 (1 being No Capacity, 6 being Highly Capable) | |
|---|---|
| **Capacities** | **Response** |
| Knowledge needed to manage an overseas market entry | 1 (No Capacity) |
| Ability to protect Intellectual Property in product and/or services targeted overseas | 1 (No Capacity) |
| Operational capacity | 1 (No Capacity) |
| Resource capacity | 1 (No Capacity) |
| Financial capacity | 1 (No Capacity) |

### Analysis

The Computer Doctor Liverpool is typical of small IT companies who support the technical requirements of individuals and small offices in their local area. By offering a comprehensive suite of

IT systems support in a service contract The Computer Doctor Liverpool has a role in every aspect of IT service provision including those activities which the UKTI has classified as cyber security.

There are many companies like this in the North West of England. Often these companies primary roles are PC repair and IT support for local businesses. Due to customer demand for security, companies like The Computer Doctor Liverpool also supply anti-malware products, design security policies, arrange local or cloud based backup systems and offer forensics in the form of data recovery. However many of these companies, including The Computer Doctor Liverpool, do not consider themselves part of the North West Cyber Security Industry. Instead they consider themselves part of the North West IT Support Industry.

It may be difficult for The Computer Doctor Liverpool to expand into overseas markets because they focus upon a limited geography. However their fast and high quality services clearly leave a good impression on their clients (see testimonials on company website). There may therefore be an opportunity for The Computer Doctor Liverpool and other PC repair/IT support companies to piggyback on the overseas expansion of their clients. For example, if a client opens new offices overseas it may be possible for The Computer Doctor Liverpool to obtain a support contract for those new offices and offer remote support which would include cyber security products and services.

Indeed a similar local PC repair/IT support company Keswick Computer Services told the research team that they support their clients wherever they are on the planet. This led to Keswick Computer Services gaining a contract to supply infrastructure and support to a client based in Cumbria who setup a chalet business in France. While the client was based in the UK it created an opportunity for the company to expand into a new business area (chalets, holiday rentals etc) and have a physical presence, at least during the setup period, overseas which could be an opportunity to create an export customer base.

# MDSec

Does not export. Wants to export.

MDSec is a security consultancy company based in Macclesfield. The company is designed to help businesses to secure themselves and to meet security standards. To do this MDSec offer consultancy services including data forensics, penetration testing and vulnerability auditing. MDSec is CREST accredited and works with CESG. MDSec consider themselves "the experts' experts" when it comes to training and education in the field of cyber security.

MDSec's business model involves assigning individual consultants on a case by case basis depending upon the needs of the customer. The consultant will perform assessments in line with CREST methodologies. While it is not explicitly stated MDSec most likely charge for the time a consultant spends on a project and for specific assessment and remediation actions.

MDSec were assessed using open source information and interview. MDSec have been a registered company for 3 years under the company number 07909398. They are registered under the SIC 2007 code 62020 0 Computer Consultancy Activities. DueDil identifies MDSec to have less than 50 employees and have turned over approximately £1.35m in 2014 based on available trade debtor information. Between 2013 and 2014 MDsec 's Assets Growth by 35.7%.

## Cyber Security Activities/Capabilities

MDSec take part in Surveillance and Reconnaissance, Information Operations, Analytics and Big Data Analysis and Forensics. They design bespoke services for each of these cyber security activities and provide services in Analytics and Forensics. Based on UKTI segmentation MDSec can be said to take part in advisory, assurance and educational work.

Much of Mdsec's specific cyber security services are elements of stress and penetrations testing which requires elements of Reconnaissance, Information Operations, Analytics and Forensics. Their major areas of advisory and assurance work include "Web application Assessment" "Code Review", "Product Assessment", "Reverse Engineering", "Mobile Security Assessment", "Infrastructure Assessment", "Database Security Assessment", "Unix Build Review" and "Windows Build Review". As part of their education work MDSec runs courses on "Application Assessment", "Application Defence Training", "Database Assessment" and "Web Application QA Training".

## Export Activity & Export Readiness

While MDSec seem to be a thriving business with a strong customer base inside the UK and a strong service portfolio they do not currently export. However MDSec expressed interest in exporting during the survey and interview phase of this study.

### UKTI Priority Markets

MDSec were asked to assess the likelihood that they would export to each of the UKTI priority markets in the future.

| The respondent was asked to rate the likelihood of entering each market from 1-6 (1 being No Possibility, 6 Certain) | |
|---|---|
| **Market** | **Response** |
| Kuwait | 2 (Very Little Chance) |
| Qatar | 2 (Very Little Chance) |
| UAE | 2 (Very Little Chance) |
| Saudi Arabia | 4 (Somewhat Likely) |
| Brazil | 3 (Little Chance) |
| India | 4 (Somewhat Likely) |
| Malaysia | 5 (Very Likely) |

Interestingly MDSec had no other planned export destination to discuss. Their positive responses to UKTI markets were prompted because individuals within the business had contacts within those destinations therefore making those markets possibilities. It seemed as though MDSec have not consider exporting systematically but are keen to expand into overseas markets should the opportunity arise. MDSec are not targeting expansion into Saudia Arabia, India or Malaysia but they feel that they would be able to export should the right project arise.

### Product/Service Exports

MDSec were asked to assess the likelihood that they would export specific products/services overseas.

| The respondent was asked to rate the likelihood of the company exporting specific products/services 1-6 (1 being No Possibility, 6 Certain) | |
|---|---|
| **Market** | **Response** |
| Sophisticated and targeted attack prevention | 6 (Certain) |
| Large scale ICT systems or services that have a significant cyber security element | 1 (No Possibility) |
| New and large scale financial services systems | 6 (Certain) |
| Research capabilities | 1 (No Possibility) |

Although MDSec do not have concrete plans to export to specific markets as of yet they are clearly certain that export activity is on the horizon. Furthermore they are clear about what they can and cannot export. Attack prevention measures cover the full gambit of MDSec consultancy services and so it is little wonder that the company is confident that they will export these services. A large number of MDSec customers are in financial services; these customers are motivated by standard requirements such as PCI DSS and the potential damage to customers should they become targets for cyber attacks. As a result MDSec is confident that they could replicate the services they administer in the UK to finance organisations overseas. However the company has no interest or capability to deal with large scale ICT systems or Research capabilities.

## Project Collaboration

MDSec were asked to assess the likelihood that they would contribute to specific types of project outside of the UK in the future.

| The respondent was asked to rate the likelihood that the company would contribute to specific types of project 1-6 (1 being No Possibility, 6 Certain) | |
|---|---|
| **Market** | **Response** |
| Sophisticated government intelligence-gathering systems | 4 (Somewhat Likely) |
| Major new communications infrastructure, including fixed-line fibre/cable infrastructure, broadcast or mobile telephony | 4 (Somewhat Likely) |
| New transport infrastructure, including ports, railways and airports | 4 (Somewhat Likely) |
| New energy generation and distribution infrastructure, especially that which includes smart metering. | 4 (Somewhat Likely) |

MDSec were cautiously positive that they would be involved in all four of the specific projects suggested to them. Once again this demonstrates the early stage that MDSec are at in the process of becoming exporters. They understand what they are capable of doing (Product/Service Export) but they do not have a clear plan for destinations or the projects on which they are likely to work. Because of the flexible and comprehensive nature of MDSec consultancy services there is scope to work in each of these projects.

## Export Capacity

MDSec were asked to assess their capacity in specific areas which contribute to their ability to export.

| The respondent was asked to rate each capacity from 1-6 (1 being No Capacity, 6 being Highly Capable) | |
|---|---|
| **Capacities** | **Response** |
| Knowledge needed to manage an overseas market entry | 4 (Somewhat Capable) |
| Ability to protect Intellectual Property in product and/or services targeted overseas | 5 (Very Capable) |
| Operational capacity | 4 (Somewhat Capable) |
| Resource capacity | 4 (Somewhat Capable) |
| Financial capacity | 5 (Very Capable) |

Evidently MDSec are positive about their ability to export to overseas markets. They are especially confident in their finances (Open source data about the company suggests that this confidence is well founded) and their ability to protect their Intellectual Property.

## Analysis

MDSec represent the majority of businesses in this study in a number of ways. As well as being a small business with highly technically skilled team members. MDSec are a registered company under the SIC 2007 code 62020. They are also a young company having been registered for around 3 years. MDSec are unusual in that they do not carry out Security Management activities as the majority of businesses in the industry do. However they represent the innovative sector of the industry who design their own products and services, as detailed earlier the innovative sector is very important to the industry.

From an export point of view MDSec represent the portion of the industry that are capable of exporting but are not yet active overseas. Their lack of engagement overseas can be attributed mainly to the short time that they have been operating. MDSec have been rightly concerned by the need to build a secure foundation within the UK before exploring external ventures. With a partnership with CESG it is clear that this foundation has been established and management are in the early stages of exploring export options.

MDSec are in an unusually strong financial position compared to the majority of the market (who turned over <£250,000 in 2014). Combined with general confidence in their ability to operate overseas it appears that MDSec are simply waiting for opportunity to present itself.

# The NCC Group

Currently Exporting

The NCC Group is a Manchester based information assurance company with 21 locations across UK, Europe, North America and Australia. TheNCC Group position themselves as a total information assurance provider which involves security consulting, risk management, software and penetration testing, web services and incident response.

The NCC Group's business model is diverse, involving both long term and ad hoc contracts for their various services. They generate income on a consultancy basis not unlike MDSec and as a result of their standard products and services. In addition The NCC Group provide a free resource centre or knowledge base via their website.

The NCC Group were assessed using open source information and interview. They have been a registered company for 16 years under the company number 03742757. They are registered under the SIC 2007 code 62020- Computer Consultancy Activities. DueDil does not hold any financial information for The NCC Group. We estimate that they have around 250 employees and that their turnover is more than £40m per year (based on conversations with NCC Group employees).

## Cyber Security Activities/Capabilities

The NCC Group take part in Security Management, Surveillance & Reconnaissance, Analytics and Big Data, Forensics and Trusted Platforms activities. They provide services in all activities as well as design, integration or products in each activity. The NCC Group are active in advice, assurance and education.

In order to create "Total Information Assurance" The NCC Group offer the following services. "Software Escrow & Verification", "Security Consulting", "Information Risk Management & Governance", "Software Testing", "Website Performance" and "Incident Response & Investigation". Managed Security Services or "Incident Response" is perhaps the most interesting of The NCC Groups services in the context of the wider industry. Such capability is the nth degree of Security Management and requires a high resource capacity in order to manage multiple systems in disparate locations.

## Export Activity & Export Readiness

The NCC Group are currently exporting and they are doing so globally through their Manchester HQ and their 20 other sites worldwide. The NCC Group website is not specific about the countries in which they sell. However the location of the NCC Group offices is known 17 offices are in English speaking countries and the remaining four are located in Switzerland, The Netherlands, Germany and Denmark. The interview with an The NCC Group undertaken as part of this study revealed anecdotal evidence of The NCC Group working in Brazil to support the 2016 Rio Olympic Games.

### UKTI Priority Markets

The NCC Group were asked to assess the likelihood that they would export (or increase exports) to each of the UKTI priority markets in the future.

| The respondent was asked to rate the likelihood of entering each market or increasing exports in each market from 1-6 (1 being No Possibility, 6 Certain) | |
|---|---|
| **Market** | **Response** |
| Kuwait | 3 (Little Chance) |
| Qatar | 3 (Little Chance) |
| UAE | 4 (Somewhat Likely) |
| Saudi Arabia | 4 (Somewhat Likely) |
| Brazil | 5 (Very Likely) |
| India | 5 (Very Likely) |
| Malaysia | 3 (Little Chance) |

The NCC Group are positive about the likelihood of exporting (or exporting in greater quantity) to UAE, Saudi Arabia and especially Brazil and India. According to their interview The NCC Group see the growing digital economies of India and Brazil as a priority for their worldwide growth. As a result they are actively pursuing more ventures in both of these countries.

In addition the NCC Group are the only subject in this study to have mentioned Japan as a specific target market for their future.

### Product/Service Exports

The NCC Group were asked to assess the likelihood that they would export specific products/services overseas.

| The respondent was asked to rate the likelihood of the company exporting specific products/services 1-6 (1 being No Possibility, 6 Certain) | |
|---|---|
| **Market** | **Response** |
| Sophisticated and targeted attack prevention | 4 (Somewhat Likely) |
| Large scale ICT systems or services that have a significant cyber security element | 6 (Certain) |
| New and large scale financial services systems | 1 (No Possibility) |
| Research capabilities | 1 (No Possibility) |

The NCC Group is clear in its understanding that large scale ICT systems with a large cyber security element are their core and most profitable services. These systems involve the real time security management services which smaller companies simply cannot support. They see attack prevention services to be a secondary set of services which they can supply under certain circumstances. However the NCC Group have no interest in dealing with financial services systems or supplying research capabilities.

## Project Collaboration

The NCC Group were asked to assess the likelihood that they would contribute to specific types of project outside of the UK in the future.

| The respondent was asked to rate the likelihood that the company would contribute to specific types of project 1-6 (1 being No Possibility, 6 Certain) | |
|---|---|
| **Market** | **Response** |
| Sophisticated government intelligence-gathering systems | 6 (Certain) |
| Major new communications infrastructure, including fixed-line fibre/cable infrastructure, broadcast or mobile telephony | 6 (Certain) |
| New transport infrastructure, including ports, railways and airports | 6 (Certain) |
| New energy generation and distribution infrastructure, especially that which includes smart metering. | 4 (Somewhat Likely) |

The NCC Group are certain that they will contribute to intelligence-gathering systems, communications infrastructure and transport infrastructure because they are already working on those projects outside of the UK. They are less optimistic about their prospects of working on energy infrastructure because the respondent was unaware of any such projects currently in the pipeline. However the NCC Group have the capability to work on such projects.

## Export Capacity

The NCC Group were asked to assess their capacity in specific areas which contribute to their ability to export.

| The respondent was asked to rate each capacity from 1-6 (1 being No Capacity, 6 being Highly Capable) | |
|---|---|
| **Capacities** | **Response** |
| Knowledge needed to manage an overseas market entry | 4 (Somewhat Capable) |
| Ability to protect Intellectual Property in product and/or services targeted overseas | 6 (Highly Capable) |
| Operational capacity | 4 (Somewhat Capable) |
| Resource capacity | 4 (Somewhat Capable) |
| Financial capacity | 6 (Highly Capable) |

The NCC Group feels that it is highly financially capable and that it is in full control of its intellectual property overseas. However the company feels that it is closer to its limit in operational and resource capacity and that local knowledge is lacking. According to the interview undertaken these

perceptions are based on their current export experience, anecdotally the NCC Group has found that its local knowledge is generally good in western markets but less so in the Middle East and South America.

## Analysis

The NCC Group is atypical of this study. If our estimations about the size of the NCC Group are correct then they are a Medium or Large Enterprise in the top 20% of the industry according to Turnover. What is more the NCC Group has grown from within the North West over the past 16 years, unlike the remainder of the top 20% of the industry who are large multinationals with business operations located in the North West. The NCC Group are therefore a major success story for the industry.

They are currently exporting around the world and targeting new markets including the UKTI priority markets. The NCC Group is comfortable with its capacity to continue to export and it is working on high profile projects such as the 2016 Rio Olympics.

The role of the NCC Group within the industry should be assessed more closely. Is the NCC Group an example of what can be done or is the NCC Group absorbing international contracts which could stimulate the medium enterprise sector of the industry which is currently lacking?

# Conclusions

The North West Cyber Security Industry is growing. This report has demonstrated that turnover has increased in the last year. Perhaps more interesting is the proliferation of businesses over the past ten years and the clear indications that they intend to keep trading and develop new markets. Furthermore the lack of notice paid to insurance and legal firms who deal with cyber security in the UKTI Export Strategy suggests that in 2013 such businesses did not form an integral part of the industry. The 120 businesses included in this study do not tell the whole story.

More than one third of companies in the industry currently export overseas. This number looks set to increase. General industry growth makes the authors confident of this observation as does data collected about future export destinations of companies within the region. This growth will be driven by international recognition of data as an asset, the fear that this asset could be lost of data and the adoption of standards such as ISO27001.

The region primarily plans to export to Europe. However the actions of the next UK Parliament may cause the industry to reconsider. 44.4% of the countries detailed by those respondents who discussed their future export plans were European. A referendum result which sees the UK exit the European Union would likely jeopardise some of those plans.

Outside of Europe there is going to be activity emanating from The North West across the globe. Other export destinations The African and South America Continents as North West companies fill the knowledge gap which is left by burgeoning economies with less sophisticated Computer Science training schemes. This international expansion will not only be technical, it will also include the ancillary industries stemming from law (particularly intellectual property law) and insurance.

There is a sense that the majority of the industry is happy to collaborate on projects across scales. This is likely explained by the complexity of IT systems which requires a willingness to interact with contractors and suppliers in order to achieve maximal outcomes. Collaboration with The UK Government is likely to come through GCHQ or The Home Office. Collaboration overseas is less clearly definable.

All export plans will have to contend with fears of language and local knowledge which were prevalent amongst telephone interviewees. Larger companies such as The NCC Group are keen to expand overseas but have been damaged in the past by a lack of local knowledge. Never the less the industries financial strength and willingness to collaborate means that these issues are not insurmountable.

The UKTI export strategy is not being followed in The North West particularly regarding Priority Markets. Most of these markets are located in The Middle East which is seen by some to be hazardous and unstable. There is some interest in India and Malaysia while The UAE and Saudi Arabia are considered the most viable of The Middle Eastern states.

The study would be furthered by greater access to the larger enterprises that refused to take part in any direct questioning.

# Appendix 1

## Categorisation of Cyber Security Companies

The UKTI report *Cyber Security: The UK's approach to exports* identified nine segments within the cyber security market. In order to establish that a company should be taken account of in this research project the company had to be fit into at least one of these nine criteria. If it did not it was not classified as a cyber-security company and therefore would not be taken account of in this project.

### Analysis Process

#### Security Management

By reading through the company website, if the answer is yes to any of the following questions the company can be categorised in the Security Management segment.

- Does the company provide Security Management services or products including the operation, installation, design, reselling or integration of anti-malware software, data backup systems or other products/services which are used in the context of securing a customer's information or computer systems?
- Does the company provide real time crisis management services?
- Does the company produce Security Management documentations or train customers in how to protect their systems or data?

#### Surveillance and Reconnaissance

By reading through the company website, if the answer is yes to any of the following questions the company can be categorised in the Surveillance and Reconnaissance segment.

- Does the company provide services or products which observe, capture and explore behaviours or identities of people and platforms on computer networks?
    - E.g. Mobile phone surveillance or real time network monitoring

#### Information Operations

By reading through the company website, if the answer is yes to any of the following questions the company can be categorised in the Information Operations segment.

- Does the company provide protection, defence and mitigation against attacks utilising surveillance and management systems?

#### Analytics and Big Data

By reading through the company website, if the answer is yes to any of the following questions the company can be categorised in the Analytics and Big Data segment.

- Does the company provide, store, retrieve, analyse or visualise very large and complex datasets?

### Social Media Analysis

By reading through the company website, if the answer is yes to any of the following questions the company can be categorised in the Social Media Analysis segment.

- Does the company capture and analyse social network activity, to establish digital profiles, understand influence, monitor trends and observer sentiment?

### Forensics

By reading through the company website, if the answer is yes to any of the following questions the company can be categorised in the Forensics segment.

- Does the company provide products or services which extract information from computer system?
- Does the company provide evidential standard computer system analysis?
    - E.g. as expert witnesses

### Transaction Protection

By reading through the company website, if the answer is yes to any of the following questions the company can be categorised in the Transaction Protection segment.

- Does the company provide products or services which allow for secure transactions of information from end-to-end in environments with variable trust levels?

### Trusted Platforms

By reading through the company website, if the answer is yes to any of the following questions the company can be categorised in the Trusted Platforms segment.

- Does the company provide especially secure hardware, often to a special standard?
    - E.g. Computer terminals, mobile phones or Industrial control systems

### Identity and Authentication

By reading through the company website, if the answer is yes to any of the following questions the company can be categorised in the Identity and Authentication segment.

- Does the company provide secure services or products which captures, stores and manages identity information, providing access and privileges?

# Appendix 2

## Capabilities of cyber security companies

To gain a more detailed picture of the North West Cyber Security Market we assessed the capabilities of companies within the industry. The companies were categorised as Service Providers, Product Sellers, Integrators or Designers.

### Analysis Process

#### Service Provision

By reading through the company website, if the answer is yes to any of the following questions the company can be categorised to have Service Provision capabilities.

- Does the company work on the basis of ongoing service contracts?
    - E.g. ongoing crisis management support
- Does the company provide education or training services?
- Does the company provide one off service contracts?
    - E.g. to perform forensics examinations of hardware

#### Products

By reading through the company website, if the answer is yes to any of the following questions the company can be categorised to have Product Seller capabilities.

- Does the company resell products or services which are owned or manufactured by a third part?
    - E.g. Anti-virus software
- Does the company sell standalone products of its own design which are sold with no service contract?

#### Integration

By reading through the company website, if the answer is yes to any of the following questions the company can be categorised to have Integration capabilities.

- Does the company integrate new products into existing computer systems?

#### Design

By reading through the company website, if the answer is yes to any of the following questions the company can be categorised to have Design capabilities.

- Does the company perform research and development which results in the creation of new products?
- Does the company create training programmes?
- Does the company carry out research?
    - E.g. Whitehat hacking

# Appendix 3

See Attached Document.

# Appendix 4

1) Do you currently export to any markets outside of the UK?
    - Yes
    - No

b) If Yes, which countries do you export to?

2) The UKTI have some priority markets that they are particularly interested in. Can you tell me how likely to you are to export to each them (or increase exports to each of them)? Please rate the likelihood of you exporting to each of these countries from 1-6, 1 being no chance and 6 being certainty.
    - Kuwait
    - Qatar
    - UAE
    - Saudi Arabia
    - Brazil
    - India
    - Malaysia

3) Are you planning on exporting to any new markets other than those we just discussed?

4) Can we use the same scale (1-6) to think about the kinds of product or services you might export in the future?
    - Attack Prevention
    - ICT systems with a significant cyber security element
    - Financial Services Systems
    - Research capabilities for universities

5) Same thing again for 4 projects you might get involved with outside of the UK?
    - Intelligence gathering systems
    - Communication infrastructure
    - Transport infrastructure
    - Energy infrastructure

6) Can you rate 1-6 the company's current capability to export based on each of these factors?
    - Knowledge of overseas markets
    - Ability to protect intellectual property overseas
    - Operational Capacity

- Resource Capacity
- Financial Capacity

NB: If there was any confusion over terminology this would be clarified by the interviewer.

**Security Futures'** mission is to is create a space where we could develop innovative techniques to think about the future, techniques that draw together the insight and expertise of researchers working across different disciplines. In this collaborative space, researchers and other partner organisations have the freedom to explore questions about security and technology. But also to formulate the questions that we might need to start asking about the emerging trends in technology, society and security. A space where we can bring together people working on the cutting edges of technology, social, legal and political disciplines to ask questions about the world we live in. A space where we might begin to imagine new horizons and start to see the problems that

**Security Lancaster** is a university wide research centre on security and protection sciences. It delivers research and education that innovates and creatively challenges the way that individuals, organisations and societies secure and protect themselves. This is achieved via engagement and collaboration with organisations from a range of sectors along with governments. The centres approach delivers the very best use-inspired and pure research alongside cutting edge education that delivers real impact and social change.

This work was funded by Security Lancaster via the auspices of Lancaster University's Faculty of Science and Technology.

## Science and Technology Business Partnerships and Enterprise

Science & Technology | Lancaster University

As well as working with a range of external partners, ICT and Security form part of a wider theme based team across Science and Technology at Lancaster who offer expertise in:

- Advanced Manufacturing
- Energy
- Environment
- Health & Human Development
- Quantum Technologies
- Mathematics and Statistics

**Working in Partnership**

Across the themes we form collaborative partnerships around these 5 key areas:

- Collaborative Research and Consultancy
- Training and Education
- Co-location and Secondment
- Student Placements
- Product Development and IPR

For more information on the research work that Security Lancaster undertakes and information on how you can collaborate with us please visit our website

**http://www.security-centre.lancaster.ac.uk**