Competitive analysis of the UK cyber security sector

A study by Pierre Audoin Consultants for
the Department for Business, Innovation and Skills

Version 1

July 29th, 2013

Pierre Audoin Consultants

www.pac-online.com

Disclaimer

This is a report by Pierre Audoin Consultants (PAC) commissioned by the Department for Business, Innovation and Skills (BIS). The views contained herein are those of PAC based on our extensive experience of monitoring the Software and IT Services market; research of open data and other resources, and interviews with over 50 individuals from industry, government and academia. Our recommendations are not intended to be binding on HMG or industry.

Contents

List of figures

Executive Summary

The UK economy depends on its cyber infrastructure in most aspects of its citizens' everyday lives. We work, play, shop, socialise, bank, and pay tax online. We save our music, photographs and personal data online. We communicate by text, voice and video online. We need our cyber infrastructure to be secure.

Cyber security, quite simply, is the set of processes and technologies that allow us to conduct business, commerce and our private lives digitally, while in a safe environment. The UK market for cyber security is worth almost £2.8 billion in 2013, and we estimate that it will be worth over £3.4 billion in 2017.

Cyber security, however, is far from being simple. The threats to our cyber environments are many and various, and they are changing on a near-daily basis. Threats to individual, corporate and government activities online[*] come from three primary sources:

- Criminal behaviour: attempts at committing fraud for (usually) financial gain;
- Hacktivism: Disrupting corporate or government activities by denial of service, defacing online content and generally damaging online reputation;
- Espionage: gathering corporate or government information illegally in order to subvert competitive advantage or national security.

The number and sophistication of threats to our cyber infrastructure are increasing daily. Numerous reports cite the increasing number of security breaches and newspapers regularly run stories of lost data files, hacked bank accounts and stolen identities.

Cyber security, then, is important to the UK's economy because it ensures our ability to conduct government, business and personal affairs securely.

The government recognises this, and has allocated £860 million towards the UK’s national cyber security strategy to 2016. This strategy is aimed at improving the protection of cyber infrastructure. The strategy also seeks to promote the UK as a safe place to do business both domestically and on the global stage, by bolstering the indigenous cyber security industry.

[*] Online, in this report, means connection to a network, including cellular and radio communications.

This report

This report has been commissioned by BIS to map out the UK's cyber security industry, and capture its dynamics. There is generally within the industry a poor understanding of the sector's market dynamics and supply structures. In short, there is an urgent need for an understanding of the competitiveness of the UK's cyber security sector, both within the UK and in comparison with other countries.

Within the broad IT sector, there are four major but inter-dependent trends that are reshaping the capabilities of technology and also restructuring the fundamental market dynamics of the industry. These trends are: cloud computing; mobility; social computing; and big data & analytics.

These four key trends are driving growth in the IT sector, and their relationship with cyber security is fundamental. Each of these trends both impacts and is impacted by cyber security and that impact can be either positive or negative. Cyber security, then, is tied intrinsically to the shape of the overall IT market.

Reading this report

This report contains substantial detail on the shape of the UK cyber security market. After our introduction (Section 1) we provide an overview of the technologies, trends and suppliers (Section 2), before exploring the market structure and size, with growth prediction (Section 3). We examine the market potential for growth in exports, and also in attracting investment (Section 4) before comparing the UK with its international peers (Section 5). We provide a SWOT analysis in Section 6 before recording our findings and recommendations in Section 7.

What does the cyber security market look like?

The market for cyber security is a varied one, and the market structure and supply chain depend on the nature of the business being protected and the extent of exposure to potential threats. For this report, we identified four separate and distinct submarkets, each of which has a different constituency of end-user organisations and supply chain players. Crossover between supply chains in the submarkets is not straightforward.

The four submarkets are:

- Defence and intelligence: this submarket is focused on securing the nation's secrets, and involves the security and intelligence agencies as well as the MoD. It incorporates the most advanced (and most secret) cyber security technologies available. It is, however, a niche market and is relatively constrained in size.

- Government, other than Defence & Intelligence: this submarket incorporates all the other government funded cyber security tasks outwith its defence and intelligence obligations. It includes security of health and education data, crime and criminal justice information, as well as more run of the mill (but essential) government operations. Although the requirements of this segment are varied and not as sophisticated as defence and intelligence, the segment is substantially larger in volume and spend.

- Enterprises: the bulk of the cyber security market is orientated around large commercial enterprises securing their day-to-day business. This would include banks, telecommunications companies, utility and energy firms, manufacturers and retailers, and its constituency comprises the largest firms indigenous to or operating in the UK. Some of these firms have a role to play in the nation's critical national infrastructure, but the nature of the threat is considerably less than that for intelligence and defence organisations.

- SME and consumers: most small and medium-sized businesses have cyber security needs, but these are substantially less in sophistication and scale to those experienced by larger organisations in government and business. Similarly, consumers do have cyber security requirements but again these are at the low end of the sophistication spectrum. We have aggregated the submarket for SMEs and consumers because the supply chains serving their needs are similar.

The purpose of identifying these four separate submarkets is not to draw hard and fast lines between them. In fact there is a degree of crossover between buyers in the submarkets in our model. The purpose is to identify the differences in supply chain structures that feed each of the submarkets. From a supplier point of view, it is vitally important to understand the characteristics of your particular market.

Clearly, selling into the defence and intelligence submarket is entirely different to doing business with SMEs and consumers. But our model shows that it is just as different selling into large enterprises as it is into the public sector (even beyond the defence and intelligence elements). The sophistication and scale of the cyber security requirements, the credentials and clearance requirements, and the way in which each submarket procures cyber security capability are all substantially different in each submarket. Suppliers to the cyber security market, therefore, need to understand the dynamics of their particular target market, and to adjust their go-to-market approaches accordingly.

It is also important for cyber security suppliers to understand the potential in their market of choice. The size of each submarket varies considerably and the predicted growth rates are also quite distinct.

The smallest submarket, but the most mature, is the defence and intelligence segment. It has been using cyber security technologies for many decades and is by far the most sophisticated user of such technologies. However, despite a common perception to the contrary, this submarket is not large, the market costs of entry (such as Commercial Product Assurance certification) are high, and the rewards uncertain. Given these factors, we suggest that this segment is the least attractive for suppliers seeking to grow their business substantially. It is also the least attractive market for new suppliers wishing to enter the cyber security space. (It remains, of course, attractive to niche suppliers with modest growth aspirations and a pre-existing track record in the segment.)

The two largest sections of the markets are the commercial enterprise submarket and the ‘other’ public sector segments. These submarkets have similar cyber security requirements and they both feature considerable scalability requirements across their organisation structures. For example, the security requirements of the DWP’s benefit payments system are not dissimilar to those of a bank. There are also similarities in the role these types of organisations play in providing critical national infrastructure.

There are differences in the maturity of elements within these submarkets: banking is particularly advanced due to its long history of security and more recent regulatory requirements. But, importantly, the skill set requirements for cyber security expertise migrate easily between these two submarkets.

The submarket with the lowest level of maturity in cyber security is the SME and consumer segment. This is significantly underserved by the cyber security industry, although this is largely driven by the low levels of demand from buyers. In fact, a major issue for the industry is the markedly low level of awareness, education and understanding of the threat to business and personal information from insufficient cyber security measures.

A particular issue for suppliers to the SME and consumer segment is the free (to acquire) or bundled nature of the basic cyber security products from Microsoft, AVG and others. It means that revenues to be gained from anti-virus, firewall and other such foundation technologies are constrained.

It is in the SME market that we think BIS needs to spend most of its attention. There are two reasons for this: driving up adoption of cyber security best practice increases the UK's stature as a safe place to do business, and increasing demand also drives the cyber security supply-side. We also think that the major beneficiaries of this increase in demand will be SME-sized suppliers of cyber security advice and services.

One of the key barriers to cyber security growth is the availability of skills. This shows up in a number of ways, from the low numbers of professionally accredited practitioners to the relatively high salaries commanded by those with experience. Limiting factors on skills include low levels of STEM graduates, a lack of attractiveness of careers in cyber security, and a disconnect between university syllabuses and firms seeking raw talent.

International comparison

How good is the UK's cyber security industry? The UK is in a competitive market, as it positions itself as a cyber security centre of expertise globally. There are many other countries that also want to position their capabilities as international leaders. What is the UK's competitive positioning against these other countries, and how can the UK best position itself both as a safe place to do business and as a centre for expertise in cyber security?

Based on an extensive analysis of the cyber security strategies in 18 different countries, our view is that the UK is in the leading ‘peloton’ of peer countries. Within this peloton are several other countries also with leading positions, and, depending on the criteria chosen, one or two countries emerge as true front-runners. But there is no break away leader in the global cyber security market.

The UK does have some particular strengths relative even to its peers. For example, the UK is internationally regarded for its respect for the right to privacy and the encouragement of a free and open ‘cyberspace’ through a supportive legal and regulatory framework. But it also has some weak areas, such as in education and skills (again relative to its peers), in which the UK government could take remedial action.

Of these actions, increasing awareness of the need for effective cyber security remains the priority. BIS, GCHQ and others have made substantial efforts in this regard, such as the 10 Steps to Cyber Security, but awareness levels remain stubbornly low[1].

Conclusions & recommendations

In our research we found that the cyber security market in the UK is sizeable and growing. But growth is patchy, and there are some areas of the market that are more attractive than others. We discovered that there are a handful of large suppliers to the market, but hundreds of much smaller players, and there are several barriers to success for these companies.

While some of the hurdles are consequences of normal market forces others are structural and can be remedied with intervention from HMG. For example, GCHQ is an acknowledged world leader in cyber security in technical aspects. But its administration of the various certification schemes lacks commercial focus.

Many smaller suppliers complain of a lack of access to government contracts, not only in the (correctly) guarded defence and intelligence areas but also in general areas such as education and local government. Part of this problem is in the procurement structure of government. But part of it is also in the dearth of business skills at the SME level more generally (not an issue specific to cyber security): many small firms lack sufficient understanding of marketing, finance and management.

We believe the biggest growth opportunity for the UK cyber security market is in the SME sector, where the addressable market is largely untapped. However, demand is also low, mainly because awareness and education is also weak. Consistent and persistent attention to increasing awareness and education amongst SMEs is essential.

In all, we make 17 recommendations, separated into those for HMG and those for suppliers to the cyber security market. These are:

Recommendations for Government

- BIS needs to be front and centre in raising awareness of the need for cyber security
- BIS should help guide businesses to a list of approved suppliers for products and services
- Accelerate initiatives to ensure we do not have a talent shortage in the UK
- Recognise and capitalise on London as the main hub of cyber security suppliers
- Boost industry credentials by publicising UK cyber security policies and agenda overseas
- Support supply-side SMEs, which are vital for growth
- BIS should expand its programme to support SMEs' selling processes
- Support SMEs in understanding their market opportunities
- Foster links between SME suppliers in the cyber security sector
- Expand initiatives to encourage more SME involvement in Government work
- Improve SMEs' exploitation of university research knowledge, IP and skillsets

Recommendations for UK cyber security providers

- Recognise that this isn't a single homogeneous market
- Be aware of the impact of the Cloud on IT usage
- Work with your peers to develop your reach and knowledge
- Look for the white space in the market
- Recognise that the defence/intelligence market is challenging
- Build alliances, partner or even merge to achieve scale

1. Introduction

1.1 THE IMPORTANCE OF THE CYBER SECURITY SECTOR

The Internet plays a big, and increasingly important role in UK life and business. 80% of UK households have Internet access, while access to the Internet using a mobile phone more than doubled between 2010 and 2012, from 24% to 51%. Around 10% of retail sales are conducted over online channels and this will rise: 87% of adults aged 25 to 34 shopped online in 2012[2]. Virtually all businesses communicate with their suppliers and customers via the Web and email, and UK Government increasingly communicates with citizens by online means.

BIS has identified that it is highly desirable that the UK has a strong, productive and competitive cyber security industry sector of its own, based on inherent knowledge, skills and capability

Increasingly, then, the UK depends on our cyber-infrastructure in most aspects of our lives: economic, cultural and social. The rest of the developed world is in a similar position, and much of the developing world is catching up fast.

Alongside that, cyber attacks have been identified as one of the top four risks to UK national security alongside international terrorism (National Security Strategy 2010). The National Security Strategy outlined the context of cyber security within the national programme of defence against threats of all types. From that overarching strategy, the UK cyber security strategy was published in November 2011, which sets out how the UK will support economic prosperity, protect national security and safeguard the public’s way of life by building a more trusted and resilient digital environment.

HMG has identified that it is highly desirable that the UK has a strong, productive and competitive cyber security industry of its own, based on inherent knowledge, skills and capability, for two complementary reasons:

1. To support the key Government objective of making the UK one of the most secure places in the world to do business in cyberspace, resilient to cyber attack and better able to protect our interests, helping to shape an open, vibrant and stable cyberspace that supports open societies

2. To take advantage of the UK’s existing capabilities and ‘brand’ in cyber security to build a successful and competitive knowledge-based industry to exploit the undoubted need for cyber security in the UK and other countries.

But it is already generally known that the industry is highly fragmented and heterogeneous. Its structure is complex and not widely understood.

In particular, there is considerable confusion and uncertainty regarding the market dynamics for cyber security, in terms of demand, competitiveness and government’s role in facilitating a strong cyber security capability in the UK.

This report by the consultancy PAC, commissioned by BIS, seeks to build an understanding of the evolving cyber security marketplace and industry in the UK and worldwide. It helps to understand where the sector is growing, and why, and how the marketplace operates. It seeks to identify and quantify the opportunities for the UK's own cyber security industry, and to give a comparative, qualitative and quantitative analysis of the UK industry in the world context: the structure of the supply side, who the leading firms are and differences between the UK industry and its counterparts in other key countries.

The report examines:

- Emerging trends and market needs in cyber security technologies and services
- The different types of buyer group, their differing needs ways of acquiring solutions
- The supplier landscape – the different types of solution provider in the market, locally and internationally: how they compare, how they are funded, how they collaborate and how they compete
- Market sizes: how the market is segmented, and how the segments compare today and how they will develop, at home and overseas
- A comparison of the environment for cyber security in different countries around the world: government initiatives, industry strengths.

These are then used to construct a "SWOT" (strengths-weaknesses-opportunities-threats) analysis for the UK's own cyber security sector.

And from this, the report offers conclusions and recommendations for BIS on how to help foster the UK cyber security industry to meet the twin goals outlined above.

2. Cyber security technologies, trends and suppliers

2.1 DEFINING CYBER SECURITY

There is no accepted definition of cyber security that is in use consistently either within the UK or globally. In fact, a recent report[3] comparing the national cyber security strategies in representative countries noted that there is "a lack of a common, harmonised definition" of cyber security, which "may be a cause of confusion between nations when discussing international approaches to the global cyberspace threats." Most attempts at defining cyber security focus on digital data and devices connected to the Internet. But some countries include internal networks not part of the Internet. Others include communications assets such as routers, switches and cellular network infrastructure.

For the purposes of this study we have used a broadly defined scope of cyber security, but we draw attention to the variability of definitions as it affects the ways in which the UK's cyber security market maybe compared with that of other countries.

The International Telecoms Union (ITU) defines cyber security as follows:

> Cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and user's assets.

Cyber space is described in the UK Government's National Cyber Security Strategy (NCSS) as "encompassing all forms of networked digital activity".

In practical terms, we include the plan, build and run of cyber security solutions that range from strategy formulation through services and software to physical cyber security infrastructure. When sizing the market (see Section 3.3) we count cyber security services and software and the related hardware, both specific cyber security hardware (such as appliances) and related non-specific hardware (such as servers that host cyber security software).

For the purposes of our market sizing we exclude identity devices, such as ID cards and biometrics passports, mobile telephony SIM cards and other security tokens. We also exclude security personnel (guards), buildings and equipment such as CCTV.

It is important to note that there are other elements of the cyber security market that are not explicitly covered in our definition and market sizing. For example, many software applications are not specifically aimed at the cyber security market, but embed secure development practices and/or features.

Indeed, there is a wider trend towards embedding security technologies in other technology products, and security is often a fundamental element in much larger system builds. Increasingly, the security dimension of a large system is hidden or at least not made explicit. This can make it difficult to truly determine the size of the cyber security market: not all of the cyber security elements are made obvious.

In general, though, cyber security should be a component built in from inception of any IT system, as it is easier to solve security issues at design stage. This integration of cyber security into most business projects is changing the cyber security landscape.

Cyber security specialists are increasingly integrated into both IT and non-IT companies. Cyber security managers report typically to a chief security or risk officer, and less to internal IT.

Cyber security is complex and has many variables and processes, so automation should be a primary goal. For example, automated vulnerability identification and remediation is a growing area, and forensic analysis and governance can all now be automated. Automation may also be a mechanism to alleviate skills shortages in the future – much of the analysis of security alerts and events is still conducted by humans.

"Cyber security is more about skills and competence than a market in its own right. Security features are increasingly embedded in systems, services and products, rather than sold as separate software or devices, except in the high assurance market where distinct assured components are likely to persist."

Paul Thorlby, QinetiQ

2.2 TECHNOLOGY TRENDS

Within the broad IT sector, there are four major but inter-dependent trends that are reshaping the capabilities of technology and also restructuring the fundamental market dynamics of the industry. These trends are:

- Cloud: the distribution of computing over a network and commonly paid for using a pay-as-you-go service charge;
- Mobility: The use of smartphones to access information and conduct transactions over the Internet. It also features exponential growth in the variety of mobile devices being connected to the Internet, driven in large part by end-users connecting their personal devices to the corporate network (a phenomenon commonly known as bring your own device (BYOD));
- Social: The use of the Internet to conduct social interactions, initially with friends and relatives but increasingly used now in the business world, to aid collaboration;
- Big Data & Analytics: The gathering of massive amounts of information and the ability to search this knowledge for importance patterns.

These four key trends are driving growth in the IT sector, and their relationship with cyber security is fundamental. Each of these trends is both enabled by cyber security and can improve the overall effectiveness of a secure environment. But they can equally have a negative impact on the security of information and processes if deployed carelessly (or maliciously). Cyber security, then, is tied intrinsically to the shape of the overall IT market.

Additionally, as more and more devices are connected online, towards the ‘Internet of things’, the scale of cyberspace, and the potential for cyber security breaches, is constantly increasing.

2.2.1 Security for the Cyber Age: from IT security to cyber security

The opening of economies, globalisation and innovations such as the arrival of PCs, cloud computing or mobility have lowered the protection of enterprise and governments’ IT security systems.

Before the Cyber Age the best IT Security systems were conceived like a medieval fortress. In a castle, external protection is impressive, doors and windows small, scarce and heavily protected, giving little and difficult access to the interior. This approach is still common amongst most enterprises and administrations.

But now, from personal to enterprise, from Web to SCADA (supervisory control and data acquisition), systems are now open and will remain open. Business and individuals demand it. The balance between business protection and business enablement is changing, to enable e-commerce: internet-based customer, partner and supplier relations. This is driving organisations to open the walls of the IT fortress.

So organisations are evolving from a traditional IT security view to a more open, more complex but more complete cyber security approach. To illustrate this overarching trend in cyber security, we can think of two tropical fruits:

- The *coconut* represents old style IT security: like a fortress, this fruit is hard outside but soft inside
- The *mango* represents the new cyber-age approach to IT security, being soft outside and hard inside.

The most secure solution would be a coconut shell with a mango core, but it will not be ‘edible’ – in IT terms it is not cost-effective, nor practical for most organisations. Nevertheless, certain specific industries and governments bodies needs totally hardened systems – giving rise to the *hierarchy of needs* we presented in section 3.1.5.

But for the majority of companies, governments and individuals that want to get the most from the digital age, the mango is the better choice. Those organisations are working to harden the core of their IT:

- Their important data, like products, clients and contracts
- Their key processes, like R&D
- Their critical applications, like finance and HR
- Other vital infrastructures and systems.

This approach to security is in fact technically well designed for cloud infrastructure, (the power behind Software as a Service (SaaS)), mobility, big data or social networks.

But cyber security requires much more than a facelift as it is a systemic approach to security.

2.2.2 Intelligence and forensics

Cyber security is a constantly moving field and needs to be effective and to constantly adapt. This makes intelligence and post-event analysis very important. It gives knowledge of past attacks and helps to counter new ones. It also includes research and development. They permit proactive actions, best practices and internal cyber security improvement.

Security intelligence software can be generic (closely aligned to general business analytics software) or very specific, emerging most often from Defence and Homeland Security software. Many of this comes from economic intelligence or defence solutions. Increasingly, security intelligence systems rely on Vulnerability Management, Asset Discovery and Management, Behavioural Intelligence and Artificial intelligence (see below).

These complex functions require much more than just software. They require specific and scarce development teams with approaches that are centred on research and development. These teams develop methodologies and custom software to analyse past attacks, and produce new best practices. R&D teams are at the heart of the technology advances, but they are very expensive to build (finding the right mix of experts and researchers) and to run. Today, most R&D is conducted within the largest commercial technology firms, and within well-funded defence/intelligence agencies (particularly in the US).

Security intelligence also needs heavy-duty computing and network equipment to watch the network. It often includes agreements with telecoms operators for equipment to be installed inside their networks hubs. Those systems are based on a central threat database that will update the security units of the affiliated companies.

Normally only the biggest organisations have internal units like this. Other companies rely on contracts with security laboratories or/and with their managed security services provider.

The governments and the supra-national entities such as the EU, NATO or Interpol have a strong role there. As they often support and subsidise research they must have the same role in intelligence and forensics. The European Union has created European CERTs (Computer Emergency Response Teams) and several governments including the UK have such organisations.

2.2.3 Cryptography

Cryptography was one of the first security systems used, and also one of the first uses for computers. It is still at the core of cyber security and its mastery is critical for any country. The main products today, which many businesses are dependent on, utilise public key infrastructures (PKI), which was invented at GCHQ in the 1970s.

Cyber-security cryptography relies heavily on mathematical algorithms designed around computational hardness (such as factoring large prime numbers) with the assumption that computing power is limited. But that assumption is being challenged, especially with the availability of high power computing power via the cloud, so cryptographic techniques must constantly evolve.

Cryptography is one of the fields where the battle between attackers and defender computing powers is the fiercest. This is because, using traditional mathematics such as prime number theory, processing power both enhances encryption and facilitates decryption: those that have the greatest computing power win.

Advances in cryptography have focused in recent years on the use of quantum computers. Although still in development, quantum computing theoretically enables the solving of traditional mathematical algorithms much faster, breaking (for now) the processing power race. Many crypto labs are focusing on perfecting and industrialising quantum cryptography.

Quantum computing is still in infancy. However, the few commercial applications that are currently available focus on encryption, due to guaranteed detectability of attempted unauthorised access (a process known as quantum key distribution systems).

2.2.4 Artificial Intelligence

Artificial Intelligence does not have a good reputation in the generalist IT market due to early promises that were not met and an innate complexity. However it has found a home in certain niche markets (such as credit card fraud detection – linked to cyber security) and IBM’s Watson is starting to find uses, such as in detecting healthcare trends. A less sophisticated but more popular example would be recommender engines as used by Amazon and Netflix (“you bought that, so we think you’d like this”).

In certain markets such as military aircrafts or space technologies AI is a hot market. It is gaining traction from automation, robotics and now from security. The first cyber security systems using this type of technologies are Defence and Homeland Security solutions such as the New York 911 CCTV systems.

Now AI is gaining ground thanks to the sophistication of cyber attacks, in particular in vulnerability and asset management and behavioural analysis. For example, AI systems can detect anomalies in system or user behaviour, which may signal cyber security attacks or fraudulent activity. It is a good example of the application of the general IT trends of big data and analytics to specific security issues.

AI needs a lot of computing power to perform well. Beyond those with the resources to deploy large scale high performance computing, AI will be provided as compute-as-a-service capability in the Cloud, with access provided to big data capacities. Quantum computing is emerging as the next source of advancement in AI, but it is not proven in industrial or commercial applications.

2.2.5 Behavioural Analytics

Behavioural Analytics is one of the hottest topics in cyber security. It has two aspects:

- Network Behaviour Analysis is an inside-security perimeter analysis that flags new, unknown or unusual networks patterns that might indicate a threat – so-called anomaly detection. It helps to lower the human analytical intervention by automating certain human duties.
- Human Behaviour Analytics, that analyses human-to-machine interactions, including what users are doing and saying. It can identify malicious intent using, for example, social networks.

"Behaviour Anomaly Detection provides the ability to detect threats that are not part of a known pattern or signature, but which are unusual or unexpected. It's vital to defend against newer or targeted attacks."

Piers Wilson, Tier-3

Behavioural Analytics are a very good addition to next generation UTM, SIEMS and Vulnerability Management systems. Few stand-alone product exists, and new functionalities are typically embedded within other software products or very specific and powerful custom developments.

Behavioural Analytics systems are often based on advanced technologies such as correlation engines, complex event processing, rules management systems or even artificial intelligence

2.2.6 Identity Management

Identity (ID) management systems are one of the main characteristics of any cyber security systems. For humans, able to recognise known individuals at a glance, identity management may seem straightforward. But for computer systems, tasked with authenticating the identity of millions of individuals, it is highly complex. It is also a primary area of attack by hackers.

ID management systems manage individual entities, their authentication, authorisations, roles and privileges. They include, but are not limited to:

- Directory Services, such as Microsoft's Active Directories
- Logical ID providers
- Digital security support (for passport, IDs, SIM Cards, ID badges, etc.)
- Software security tokens
- Single Sign On

Software ID management systems are mostly supplied as software suites from the major systems management software vendors from the US. Their typical target audience is the IT divisions of larger generic businesses and governments.

Defence contractors provide more global ID management systems that include also all type of digital IDs. They could have their own technologies or white label other technologies as part of their ID management platform. Their targets are governments and specific industries: transportation, energy, defence.

Logical and digital ID management are converging as suppliers tighten their cyber security portfolios.

Identity Management will increasingly rely on smart devices (smartcards, tokens, etc.) as multi-factor authentication, and will be combined with claims-based identity (from Microsoft) and biometrics (see below).

2.2.7 Biometrics

Although the market for biometrics sits outside our definition of cyber security, traditional ID management has reached its limits both in complexity and protection capacities. Increasingly, those systems are completed with biometrics, and so we have included this brief summary of the application of biometrics in access control systems.

Biometrics are systems that identify humans by their physical characteristics instead of token based systems such as a password or an ID number. Fingerprints were a commonly used approach, but now iris and retina recognition, and even DNA sampling techniques are being deployed. They can also identify individuals by behaviour patterns such as voice and keyboard typing patterns. These systems are very intensive in algorithmic processing to detect, analyse and alert administrators, according to certain specific rule sets. Biometrics are most often used in conjunction with other ID systems.

Biometrics have been beset by many practical issues over the years, not least of all user resistance to initialising processes such as fingerprint and facial scanning. It is also prone to false reject rates that, while are well within statistical norms, have the capacity to annoy the users (where the system fails to authenticate a valid individual).

The next advance in biometrics is DNA testing. It is attractive because the identifying attribute does not change over time (unlike many physical characteristics). DNA biometrics are currently costly and takes too much time and effort to deploy commercially. However, DNA profiling costs are plummeting and may soon be commercially viable.

2.3 SOLUTION TRENDS

2.3.1 Risk Management

Risk management is now a key catalyst for cyber security. Industry, financial and state regulations are at the core of Risk Management. Risk Management is strongly linked to internal and external audit functions.

This financial approach to cyber security is quite new and resources are scarce, as it requires a cross-functional view: business, IT, cyber security and their financial implications, are involved, and multi-disciplinary teams are required. Few software tools exist that encompass cyber security risk as an input to measuring exposure. Most

"Fear is not the way you win this (adoption) war – business continuity, not fear and regulation, will convince companies to (implement cyber security).
Stuart Aston, Microsoft

organisations do not have internal teams and there is a big market for sub-contracting companies to plan, build and run such organisations

2.3.2 Vulnerability Management

Vulnerability management has become a must-have in the field of cyber security. Originally vulnerability management was static, a periodical audit of your defences according to known threats. But cyber security is an increasingly fast moving environment, and vulnerability management is now a permanent feature of cyber security systems.

Vulnerability management systems must be high performing, so as not to impact performance, and the threat and vulnerability database must be accurate, with updates being supplied from a remote or regularly refreshed database.

Vulnerability Management is delivered by three types of provider:

- Cyber security auditing companies that conduct whole cyber security audits with several sets of software tools
- Cyber security suite vendors that include this feature in their software
- SaaS providers, providing VM via the cloud.

The SaaS providers have been growing quickly and are overtaking the other players. But strict attitudes to data localisation are challenging this, since those players normally store vulnerability registers offshore in their datacentres. Providers are moving to a hybrid model that more closely reflects that used in security intelligence: data stays local, but systems are updated online.

2.3.3 Asset Discovery and Management

It is difficult to secure and assess the vulnerabilities of a system if its components or assets are undocumented. Like vulnerability management, to which it is closely linked, asset discovery and management is essential.

Asset discovery and management (ADM) is at the intersection between IT security and system management. Cyber security requires both security specialists and system management expertise. Cyber security is not an isolated market: it impacts all other IT markets.

Systems management is not a traditional strong point of IT security specialists and so some collaboration with, or acquisition of (or by), IT management specialists or mobile device management players is likely.

Interestingly, specialist European software companies are strong in this segment as specialists, and there are also some Open Source alternatives.

Advances in ADM lie in artificial intelligence that enable or enhance reliable autonomous systems, which cope with the complexity and heterogeneity of today’s modern systems. Like other autonomous systems, ADM will increasingly be deployed as Cloud services.

2.3.4 Mobile Security

End-point security is evolving very rapidly with the surge of mobility. In the majority of our IT manager surveys, mobility is seen as the biggest threat for IT security. The advent of BYOD (Bring Your Own Device) is merging professional life with personal life with deep security implications. Furthermore, some systems such as Apple or Blackberry may store data overseas, which may contravene local legislation.

Specialist mobile device management (MDM) software players are currently leading the way. IT security software vendors are also targeting this market with new solutions. Defence contractors are also well positioned in this market with high level solutions, featuring deep encryption levels for critical industries and governments.

New features in MDM include: content protection and erasing, sandboxing, patch management, encryption, and localisation. Some specific industries and a number of governments favour Android-based mobiles as their open source system permits customisation to adapt them to the highest security levels. This has not been the case so far in the UK, with Blackberry's proprietary system being preferred.

"There's massive growth in Unified Threat Management, mobile device management, and advanced remote working."

Ollie Hart, Sophos

A simple way to secure a device is the adoption of a Universal Cloud Client, whereby minimal data is stored on the device, and computing is most often done remotely. These solutions are spreading quickly inside larger companies as they require considerable upfront investment, with network and device security software. And they do not completely remove the risk associated with mobile devices, as they essentially shift risk away from the device and onto a remote server. But they lower management costs and permit device independence.

2.3.5 Critical Infrastructure/Industries/SCADA protection

The Stuxnet attack on the Iranian nuclear plants in 2010 demonstrated that manufacturing, energy and utilities firms are vulnerable to cyber attacks. It showed that threats are not simply aimed at financial gain, but can sabotage critical infrastructure too.

Critical infrastructure ranges from highways to nuclear plants, including water treatment, airports, railroads, power grids and emergency services. Some of them, like airports, railroads or ports authorities are already very secure due to anti-terrorist regulations. The main cyber security providers to these organisations are defence contractors. But for other industries with plant, threats such as Stuxnet that target the production SCADA systems are a dangerous threat.

Such systems often use specific programming languages, elderly versions of software that are poorly documented, or are based on older and unsupported versions of Microsoft software. Securing them retrospectively is not easy, but for companies who need to secure their operations, it is a necessity. This is opening up a very interesting and dynamic market, but it tends to be very localised and industry specific as it relies heavily on specialised IT services.

2.3.6 Secure-by-design development

Cyber security has often concentrated its efforts on defending the perimeter and the devices, but nowadays attacks are increasingly targeting application layers. To secure an application that was not designed to be secure is difficult, time consuming and expensive.

Many companies are beginning to develop “secure-by-design” applications, starting with their most critical new applications. This best practice is already mandatory in certain industry especially those involved in embedded, industrial, technical and scientific software like defence, aerospace, energy, hi-tech and spreading to telecoms and finance.

This market is closely related to software testing, with software development platform vendors leading this market along with Open Source software.

2.3.7 Governance systems

SIEM (Security Incident & Event Management) systems analyse and correlate all events occurring in the organisation. SIEM tools have mainly emerged from the US, though some European companies like Cassidian (who manage the British Army SOCs) have developed their own technologies or are white-labelling US-originated software.

Governance, however, goes beyond SIEM:

- Business knowledge is critical, to align cyber security governance to the specific threats of the businesses.
- Security processes and procedures must be in place
- System assets and vulnerabilities have to be evaluated
- SIEMs need to be fed with event and incidents to analyse, so they rely on an already existing and mature IT and cyber security architecture.

2.3.8 Security Operation Centres (SOC)

Governance generally leads to an integrated cyber security system, the SOC. Likewise, the SIEM is at the core of the SOC, but it has also these extra functions:

- Asset & Vulnerability Management
- Intelligence & Forensic Analysis
- Incident & Event Management (detection, analysing and handling)
- Alerting

- Reporting.

SOCs permit better cyber security governance and holistic approach of the threats. They are beneficial at several levels:

- Audit reporting, as compliance becomes mandatory in certain industries such as finance
- Business continuity and risk management
- Visibility of all the layers of cyber security.

SOCs are increasingly managed outside the IT department, under the auspices of a Chief Security Officer. They are also under scrutiny by finance and legal departments, due to their possible implication in case of severe cyber security incidents.

SOCs are labour intensive, especially at the Incident & Event Management level. They often require large teams (20+ people) and large investments in secure buildings, in software, as well as important operations costs.

SOCs delivered through managed services are becoming common:

- Large companies generally source their SOC from third party solutions, and use some outsourced services such as vulnerability management or cyber security intelligence
- Other companies manage internally some parts of the SOC, the rest being outsourced
- A few companies totally outsource their SOC

The concept of a SOC is relatively new, and most firms – even large multinationals have yet to implement cyber security in this way. However, we think that SOC adoption will be one of the fastest growing areas with cyber security.

2.3.9 Managed Security Services (MSS)

Traditionally, organisations have been reluctant to outsource security functions. But the sheer complexity and extent of cyber security makes managed security services increasingly desirable, even a necessity. And as the US, French, German and British armies outsource their SOCs to (selected) third party defence contractors, commercial and government organisations will be reassured as to the effectiveness of the model, in terms of levels of service, costs and efficiencies, as well as security capability itself.

As in any outsourcing model, MSS must be carefully planned and managed, and must be designed to be fully reversible. Most companies outsource functions they cannot fully master like security intelligence. Others outsource their security infrastructure management while keeping SOC management in-house.

For many SMEs, managed security services will be the only way to become fully secure, and many such services will be adopted via cloud solutions.

The MSS market seems to be structured at the European level since service providers have their SOC capabilities within the continent and that satisfies EU data protection laws. Providers are generally the IT service market generalists, plus the security and defence contractors.

2.4 A FRAGMENTED SUPPLIER COMMUNITY

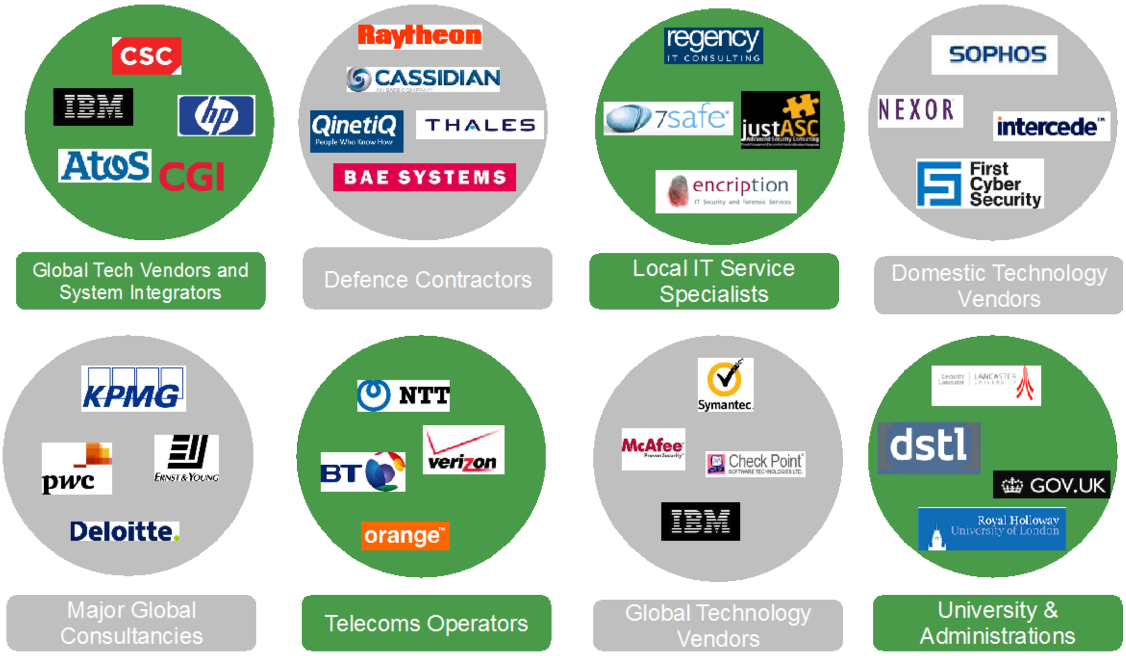


Fig. 1: A diversified cyber security ecosystem (with example firms shown)

The supplier community operating within the cyber security sector is both complex and fragmented.

It is complex because for many vendors, cyber security is not something that they provide in the form of a discrete product or service, but it is something that is included/ inserted into their wider offering.

For example, Microsoft is by no means a cyber security company, but it invests heavily in ensuring that it has a team of consultants who oversee the implementation on its products in secure environments such as defence and intelligence.

Similarly, Dell is best known as a provider of servers and storage systems, but systems and network security is a key focus area for the company as it looks to adapt to a cloud-centric delivery model – highlighted by its £400m acquisition of SecureWorks in 2011. Intel's £5bn takeover of McAfee in 2010 can be viewed as part of a long-term play to move security to the level of the CPU.

Another important characteristic of the cyber security supplier community is that its reach stretches outside of the traditional IT products and services vendors. Cyber security vendors can be broken down into eight different groups:

- **Global technology vendors & systems integrators**: Global IT giants such as IBM or HP have reinitiated their security strategies. Services generalists such as CSC and CGI have security established in their IT infrastructure practices, as most projects include security, e.g. building a universal client, exchange platforms, infrastructure-as-a-service etc. CGI Group now ranks as one of the largest providers of cyber security services in the UK following its acquisition of Logica in 2012, which delivered systems integration and outsourcing engagements in secure environments such as central intelligence, defence and national policing agencies.

- **Defence contractors**: In specialised areas such as biometrics or encryption, defence and homeland security specialists, such as Northrop Grumman, Thales or EADS, are very active. Players from this market also sell pure software solutions or virtual appliances. Their military involvement and specialist defence knowledge are crucial to the Defence & Intelligence segment, though they are also keen to generalise their propositions in order to reach the commercial sector.

- **Local IT services specialists**: There is a very large community of small, local services companies focused on providing cyber security expertise to public and commercial sector organisations. As we shall see, the majority of these companies are very small in scale (typically less than 50 employees and <£1m annual revenue), and generate much of their business on the back of the networking contacts of senior management figures. Another important sub-group within the market are value-added resellers of cyber security products. These companies are generally increasing their services delivery capabilities in order to offset declining margins on evermore commoditised equipment. For example, Maidstone-based SecureData is aiming to become a £50m-revenue company by ramping up its security services capabilities, highlighted by its purchase of application and data centre security specialists Quadrant Networks in 2012.

- Domestic technology vendors: Sophos is the best known cyber security product vendor, but there are many others. Most are small, niche firms but several have innovative technologies that promise market leading potential. Some firms are spin-outs from university research.

- **Major global consultancies**: Many of the leading management and business consulting groups have established cyber security advisory arms as their clients in both the public and commercial sectors see external help with their security strategies. For example, KPMG has more than 200 information security experts based in the UK.

- **Telecoms operators**: Telcos have invested heavily in cyber security. The link between security, cloud and mobility are strengthening their positioning and security is one of their assets to invade the IT landscape. For example, BT's Assure division pools together more than 1,800 security consultants, architects and designers worldwide.

- **Global technology vendors:** ranging from multi-billion international players (e.g. Symantec) to small and local specialists. Software giants such as Microsoft, SAP, Oracle and Dell are also important in this market by integrating security features into their products and by acquiring security software companies.
- **Universities & administrations**: these act to regulate and encourage the market by injecting R&D capability, skills and overall strategic direction.

The cyber security market will only become more diverse over the next ten years as a much greater array of devices become inter-connected and the targets for cyber attacks evolve.

For example, manufacturers of supervisory control and data acquisition (SCADA) systems such as ABB and Siemens will increasingly need to be considered as part of the cyber security universe as they build greater security defences into their systems in the wake of the Stuxnet attack of 2010, which targeted industrial systems.

Security will also be a crucial component of the UK's planned national roll-out of smart energy meter devices, which is set to commence in the next two years. Meter device manufacturers, network equipment suppliers and central market systems operators all have layers of security technology built into their offerings.

And the proliferation of cloud-based delivery models will see the burden of security shift away from clients securing on-premise applications, and back onto the suppliers of software, infrastructure and platforms at the level of their delivery centres. If a business is using cloud-delivered accounting or sales automation software on a pay-as-you-go basis, it will not expect to invest in additional hardware, software or services to ensure that the service is secure.

2.4.1 Size and Scope of UK Cyber security Suppliers

To support our analysis of the structure of the UK cyber security supplier market, we compiled a database of more than 600 key players. The companies were drawn from a number of different sources:

1. CESG approved services and products suppliers (CAPS cryptographic products; CPA commercial products; common criteria & ITSEC products; CHECK IT health check companies; CIR cyber incident response companies; CAS certified services; and CLAS consultants)
2. Intellect security group members
3. Regional cyber security/IT associations (Malvern, Cambridge)

4 Exhibitor and attendee lists for major UK cyber security events (Infosec, etc.)

5 PAC's ranking of leading UK software and IT services suppliers, based on more than 10 years of research in this area.

The main characteristic of the UK cyber security sector is that it is highly polarised between a small group of large suppliers, and a much bigger community of smaller companies (Fig. 2:), which includes large suppliers with a small share of revenue derived from cyber security. In fact, this is broadly true for any large market, and is certainly the case for the generic IT market in the UK.

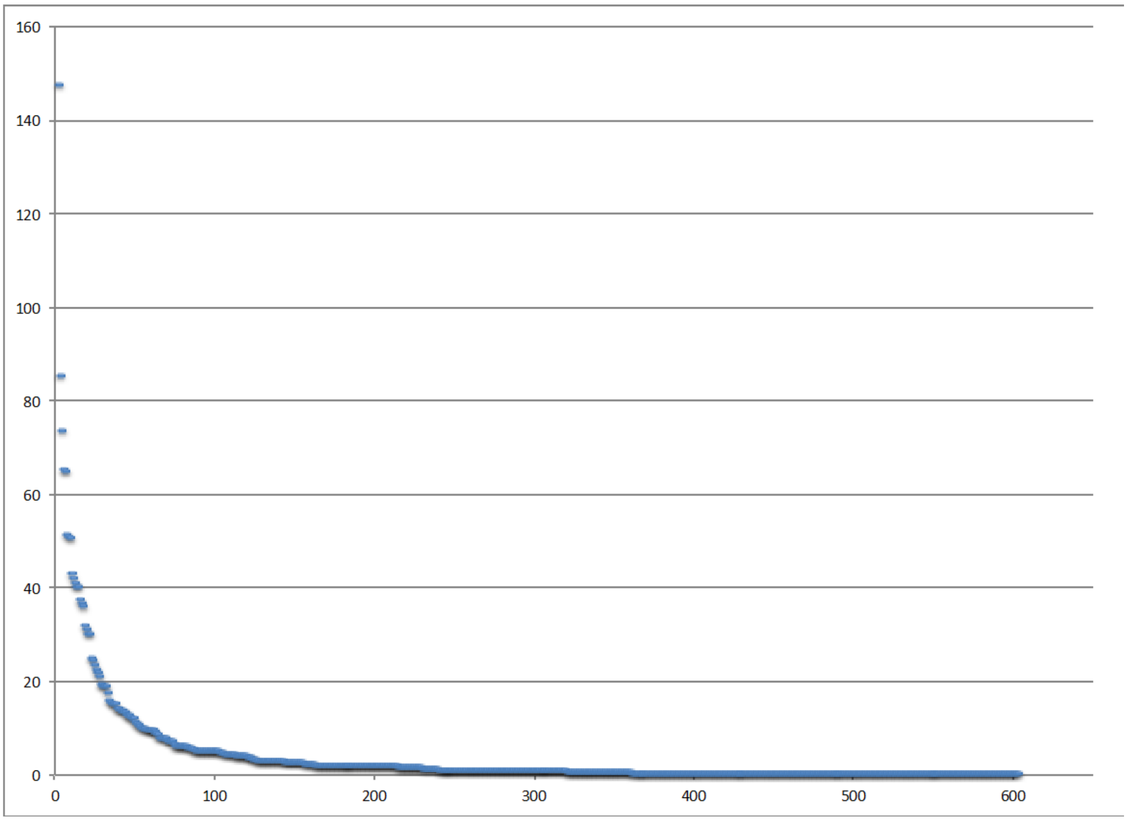


Fig. 2: Cyber security suppliers by revenue (£m)

Of the 600 companies we identified as above, only 1% had UK cyber security-related annual revenue in excess of £50m, while a further 8% fitted into the revenue band of between £1m, to £49m. The largest group (49%) sits within the £1m to £9m group, with the remaining 40% falling under the £1m sales mark, which emphasizes that this is a market that is dominated by smaller suppliers in terms of number, but by large suppliers measured by revenue.

It also means that the supplier community is much more fragmented than it is in other mature areas of the technology sector, such as desktop computer manufacturing or, to a lesser extent, IT outsourcing. It makes it a challenging supplier market for buyers to navigate, with few big brand names, and a lot of companies whose coverage is highly regionalised.

There are several firms that have substantial revenues, but only a fraction of that comes from cyber security. Major IT firms like IBM, HP and Microsoft all attract cyber security revenues less than 5% of their total income.

Almost three quarters of the 600 companies (73%) were small services companies rather than product-oriented companies. This is also reflected in the types of supplier that have gained accreditation from CESG, with more than 300 services firms having one or more 'CLAS' accredited consultants.

The majority of cyber security services business tends to be project rather than managed services, with a strong emphasis on consulting. The externalisation of cyber security services is being driven by skills challenges as much as cost or risk management. The most common focus areas for cyber security service providers in 2013 are penetration testing, security compliance audits and security process and technology consulting.

However, one major emerging trend is a growing overlap between cyber security product suppliers and services companies. For services companies, developing IP represents an opportunity to differentiate their services capabilities, and to serve as an armour-piercing tip to help them drive revenue from related advisory and managed services. A good example of this trend is Malvern-based security consulting firm Helyx, which has developed a system to help customers analyse data held in geographical information systems.

The UK cyber security supplier community is truly international. US companies account for the largest share (by revenue) of the £2.8bn market, accounting for 43% of the total. UK-headquartered suppliers account for 37% of total spending on cyber security in the country, with the remaining 20% split between suppliers from France (6%), Japan (4%) and locations as diverse as Brazil, India, Israel and Russia.

But if we look at the UK supplier community in terms of the number of companies, almost three quarters (74%) were headquartered in the UK, ahead of the US with a 16% share. However, the majority of the larger suppliers are headquartered outside the UK, while most of the domestic players are small in size.

2.4.2 Location of cyber security suppliers in the UK

PAC analysed both the headquarters and major secondary delivery locations of cyber security companies operating in the UK, and given the large number of small businesses in this sector it is unsurprising that the picture that emerges is one of a widely spread supplier community.

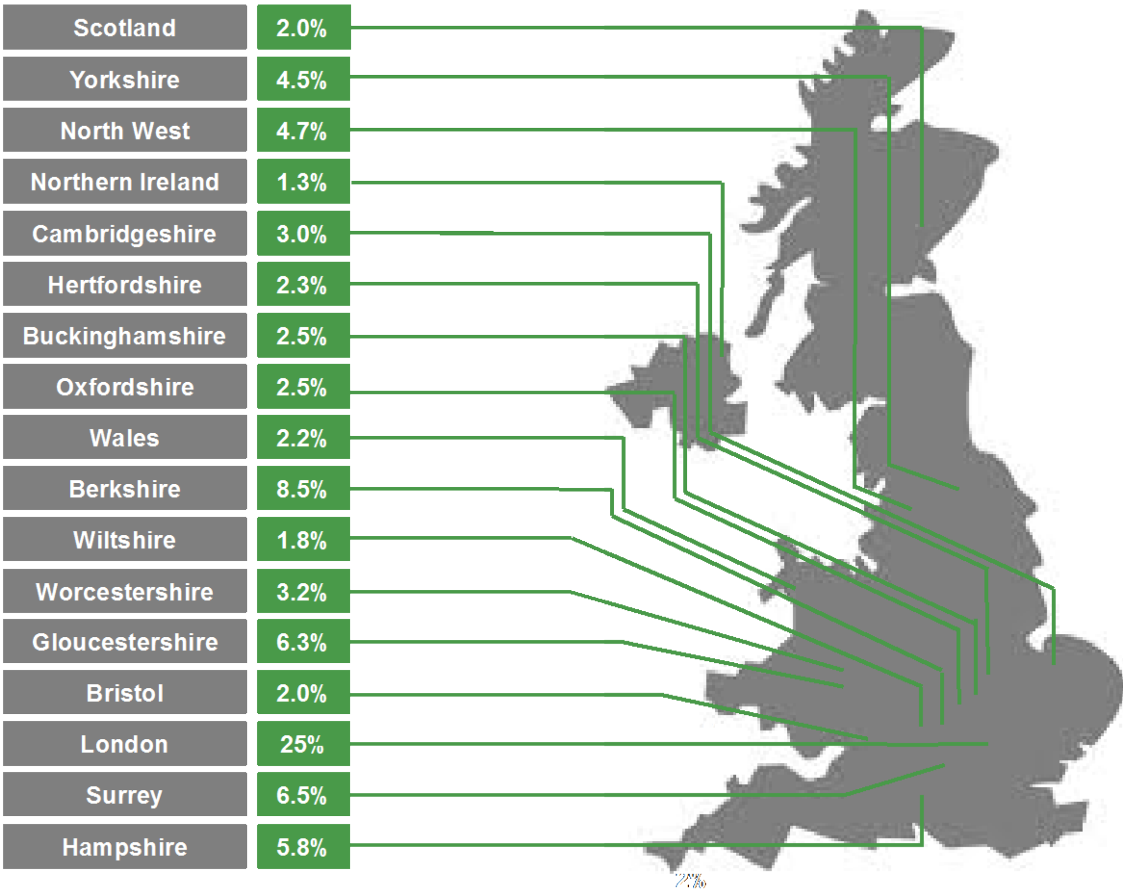


Fig. 3: **Cyber security companies by location**

In Fig. 3: we map the key headquarters and delivery locations of 600 cyber security providers. There is a considerable spread: we also acknowledge that an office location does not necessarily equate to the volume or location of services delivered. However, some hubs do emerge.

London: The capital is home to the largest number of cyber security companies, with almost a quarter of cyber security firms having a major presence in the city. While there are emerging hubs for technology companies in the Old Street and Olympic Park areas, most of these companies are based in the City, West End and Docklands areas in order to target companies in the financial services and government sectors.

Some of the firms in London are the UK offices or headquarters of large firms that have a cyber security capability, such as Deloitte and BT. But there are many specialist cyber security firms that are also located in London, such as Mimecast, BeCrypt and Portcullis, and a host of small services firms.

Berkshire: The M4 corridor has long been the choice for US and other international software companies as the location for their UK and European head offices. Suppliers such as Microsoft, Oracle and Symantec are all based here, but the county is also home to a clutch of small domestic cyber security specialists such as Assuria, a developer of security incident and event management (SIEM) technology, with close ties to Reading University. Within the county, the main centres of cyber security activity are Bracknell and Reading.

Surrey: As with Berkshire, the prominence of Surrey in our mapping of cyber security vendors reflects the large number of large technology companies that have established UK and European bridgeheads in the region. The county's cyber security hotspots are Guildford and Camberley, with the latter a base for a group of small consulting firms including Wildwood Response and CyByl Ltd.

Gloucestershire: GCHQ serves as both a magnet for cyber security suppliers wanting to sell their products and services, as well as a source of expertise that has gone on to set up cyber security businesses in the surrounding area. The likes of BAE Systems Detica and Cassidian both have a major presence in the area, but the cluster extends beyond the boundaries of Gloucestershire proper to include Tewkesbury and Malvern northwards, and southwards to Bristol.

Hampshire: This is the fifth main hub of cyber security activity, and draws on the strong Ministry of Defence presence in the county. The county is home to a number of large defence contractors (BAE Systems, Northrop Grumman) and is also the UK base of a number of big technology generalists (Nokia, Serco). There are also more than 15 specialist cyber security consulting houses located in hotspots such as Basingstoke, Fareham and Farnborough.

2.4.3 Cluster benefits

What opportunities are there for companies based in these hubs to capitalize on their proximity?

One good example is the Malvern cluster in Worcester, where a group of small suppliers based in the town collaborate on shared marketing initiatives (such as exhibiting under a shared banner at the InfoSec event), which enables them to punch above their weight in terms of brand awareness. This initiative is very much driven by a couple of enthusiastic and motivated individuals, and the presence of such people is the key to the success of these collaborative programmes.

One potential benefit of the hubs is to get a group of smaller local providers to engage with small and medium sized businesses, who are perhaps the group in greatest need of education on cyber security, and also the source of greatest commercial potential for smaller users. For example, four of Worcestershire's leading IT and cyber security organisations held a free cyber security event for SMEs last year. Local insurance business Sutcliffe & Co, Worcestershire University's Business School and Worcestershire County Council sponsored the event, which was opened by local MP Robin Walker.

There is scope to build on some of the wider regional technology associations, such as the Cambridge Hi-Tech Association, which is an association of small suppliers and individuals in the Cambridge area. As well as providing networking events on subjects that include cyber security, the association also has an online directory of members.

The ability for small companies to quickly and easily identify a local supplier that can provide proven expertise in the area of cyber security will be an increasingly valuable resource.

3. Market trends, sizing and forecasts

3.1 SEGMENTING THE MARKET BY BUYER ORGANISATION

PAC's research has identified that there are four distinct buying groups for cyber security solutions, with different buying points and behaviours, as depicted in Figures 4 and 5. These 'submarkets' are:

- Defence & Intelligence, which is a specialised sub-segment of the wider public sector cyber security segment;
- Government, other than Defence & Intelligence, which includes central and local government, publicly funded agencies, and so on;
- Large enterprises, private firms with more than 250 employees;
- SMEs & consumers, which account for the remaining private sector buyers.

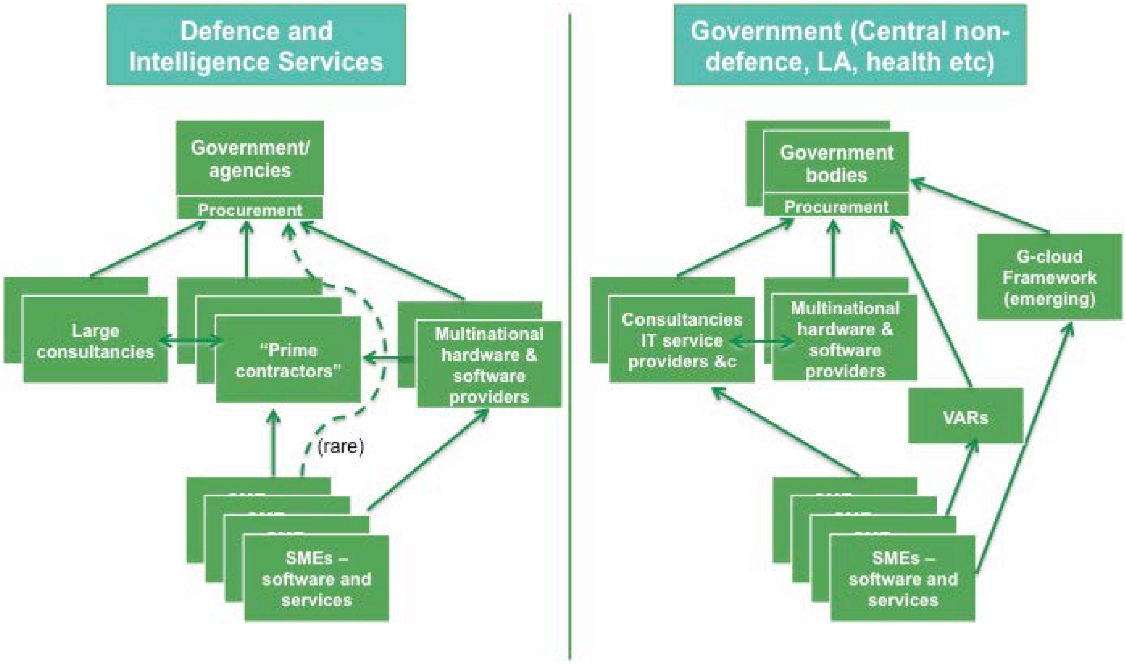

Defence and Intelligence Services
Government/ agencies
Procurement
Large consultancies
"Prime contractors"
Multinational hardware & software providers
(rare)
SMEs – software and services
Government (Central non-defence, LA, health etc)
Government bodies
Procurement
G-cloud Framework (emerging)
Consultancies IT service providers &c
Multinational hardware & software providers
VARs
SMEs – software and services

Fig. 4: Understanding the market by solution buyer type/channels to market (public sector)

It is very important to any company offering cyber security products and services to understand how the market operates in those different market segments, and the differences between them. It is equally important to Government and policy makers, in understanding how to work with those solution providers.

Success in one type of submarket is of surprisingly little consequence for companies seeking success in another market group. So for instance, key decision makers at enterprise customers operate in a different and separate community to those in the public sector. Links to the military are not particularly helpful for go-to-market and sales efforts in private companies. Selling to small SMBs and consumers requires an online and off-line, multi-tier "channel network" and is quite different to selling to large enterprises. Importantly, established vendors in specific submarkets have strong channels and alliances in place that create significant entry barriers to those trying to cross over from one submarket to another.

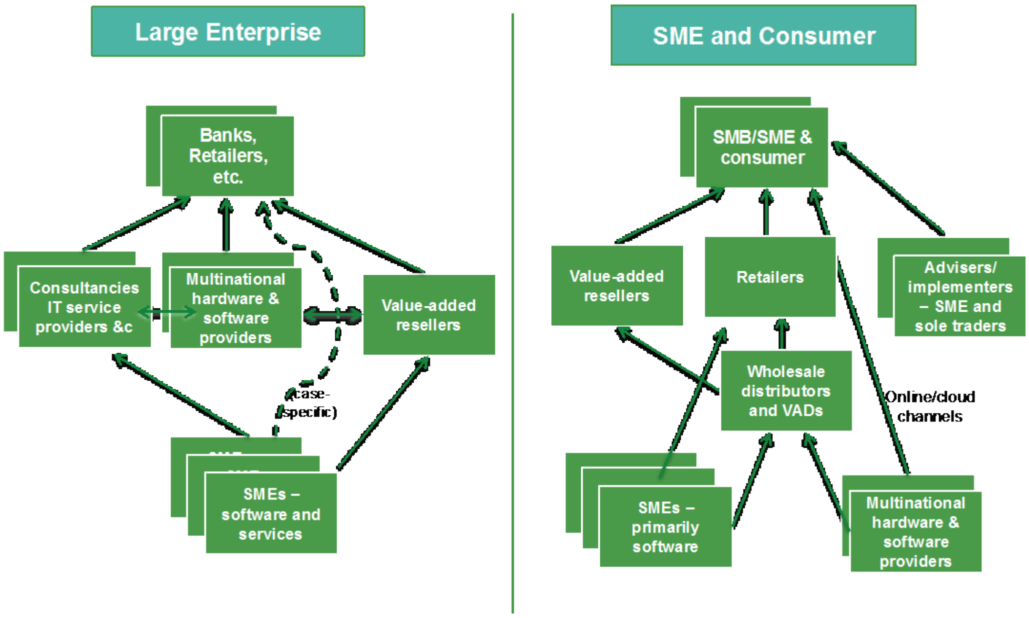

Large Enterprise
Banks, Retailers, etc.
Consultancies IT service providers &c
Multinational hardware & software providers
Value-added resellers
(case-specific)
SMEs – software and services
SME and Consumer
SMB/SME & consumer
Value-added resellers
Retailers
Advisers/ implementers – SME and sole traders
Wholesale distributors and VADs
Online/cloud channels
SMEs – primarily software
Multinational hardware & software providers

Fig. 5: Understanding the market by solution buyer type/channels to market (private sector)

Because of the different buying behaviour and delivery channels, companies need to approach each submarket differently in their "go-to-market" strategy: that is, companies need a submarket specific approach to:

- Identifying prospects, publicising and selling their capabilities – both products and solutions
- Contacting prospects (direct/indirect) – including signing up suitable partners for technology alliances and resale

- The messages that they use to highlight the attractiveness of their offerings
- Identifying and evaluating the competition they will face in their chosen market sub-segment.

Each of these aspects of go-to-market differs significantly across each of the different buying segments. Success in one does not go very far in making inroads into another.

The requirements for certification in cyber security also vary, from CLAS in the Defence & Intelligence submarket to (typically) no accreditation in the SME & Consumer submarket.

3.1.1 Defence & intelligence

With the most demanding requirements, defence & intelligence organisations buy expensive, complex products that have been accredited by bodies such as CESG or NATO, and buy services from organisations with top security clearance levels. Sales cycles can be lengthy, as procurement can be susceptible to changes in regime, funding or strategy on the buy-side. Importantly they generally buy from a relatively small group of prime contractors (typically large IT services generalists or defence contractors). These therefore provide the main market access point for smaller suppliers who find it difficult to get the attention of the big government buyers, or for whom the cost of sale would be prohibitively high.

These organisations sit right at the top of the needs hierarchy in cyber security (see Fig. 4, below).

3.1.2 Government (excluding defence/intelligence bodies)

We have grouped the non-defence/intelligence public sector organisations together as a single entity – the “rest of the public sector” – as these bodies typically do not require the same level of security assurance as Defence & Intelligence.

Of course there are significant differences within the group. This segment can be further broken down into three sub-sectors each with their own different requirements, as follows.

- Central government agencies have sophisticated cyber security requirements, particularly those agencies handling sensitive citizen data such as the Department of Work and Pensions or the Ministry of Justice. Cyber security has tended to be baked into some of the large transformational programmes such as Universal Credit, rather than sourced as a discreet function.
- Police work can also be viewed as a market in its own right. Central cyber crime bodies have very specific product requirements to help them identify, tackle and prosecute perpetrators of cyber attacks, fraud and other serious cyber offences. While some of the IT services generalists and defence contractors are active in this space (CGI, Northrop Grumman), there are also some small specialists focused solely on this market segment.

- Local government agencies, universities, health trusts etc. have not typically invested in cyber security products and services to the same extent as these other areas of the public sector. Budget pressure has meant that technology spending has been in decline in this space for the last five years, but they are also being attracted by the commercial flexibility offered by cloud delivery models. This poses both challenges and benefits for cyber security, as it both transfers some of the onus on security onto the cloud service provider, but also poses new hurdles in terms of secure integration into existing systems, and governance. For example, if employees leave the local authority, does the HR department ensure that those individuals are no longer able to access secure cloud-based services?

What links these areas together in a coherent group is their need to follow government processes for procurement, being subject to EU rules and central government mandate in their solution seeking (e.g. to buy more from SMEs). Thus selling into all of these requires particular knowledge of government procurement processes – such as the G-Cloud and OJEU – something that many suppliers, particularly the smaller ones, either do not possess or desire.

3.1.3 Large Enterprises

Large enterprises – banks, oil companies, large retailers and so on – have similar security needs (in levels of sophistication) as central government, but often with superior in-house IT skills. Their procurement procedures however are likely to be somewhat different.

They fall into two camps: the ‘vulnerable’ service providers – such as banks, card processing companies, pharmaceutical and IT service providers – who are particularly prone to attack due the nature of their business; and ‘the rest’, such as retailers and manufacturers. The first group does have more stringent security requirements, albeit less so than Defence & Intelligence.

For suppliers, the key to successfully operating in the large enterprise sector rather than, say, defence and intelligence, is to understand the level of cyber security risk that buyers are prepared to accept. For example, online retailers are highly reluctant to implement any security measures that could negatively impact the customer experience, and will carefully weigh up the cost of potential attacks (a few hours website outage) against the wider impact on their business (frustrated customers move to a rival website).

In order to do this, vendors need to have the level of vertical industry domain expertise that enables them to go beyond selling technology to articulating how their products and services can help customers tackle their challenges at a business process level.

3.1.4 Small-medium businesses and consumers

Small and medium-sized businesses[†] are the great uncharted territory of the cyber security landscape. It is dangerous to assume that because they do not have the budgets or internal expertise of large enterprises, that they do not form a market in need of cyber security support. A growing proportion of small companies are basing their business models on digital channels, as the most cost effective way to reach a large potential audience.

This has the impact of opening SMEs up to a greater risk of disruption if they are attacked, coupled with an extended exposure to attack. The 2013 Information Security Breaches Survey[4] has shown that 87% of small businesses across all sectors experienced a breach within the last year. This represents an increase of over 10% from 2012.

> "Many companies struggle to determine where to turn to for good cyber security. This is a complex domain with many competing suppliers and limited direct guidance. Government has catalysed a number of schemes; however more needs to done to identify best practice and to help potential buyers validate the claims of many cyber security suppliers."
>
> **David Garfield, BAE Systems Detica**

SMEs have completely different buying behaviour to larger enterprises[‡]. They do not typically have any dedicated cyber/IT security skills within the business and tend to buy their IT from a local reseller, from a high street retailer, or over the Web.

This physical proximity is very important as, while the products and services offered may be relatively limited, resellers remain a crucial channel-to-market for cyber security products suppliers looking to tap into a SME customer base, as the clients tend to stick with providers over a long term. Even in the age of cloud-delivered services, SMEs would look to resellers to recommend and implement/configure suitable solutions thanks to their superior skillsets and knowledge.

Also important to SMEs is buying in pre-secured services – such as email that is scanned before download (now a feature of most webmail systems like Google), or external secure payment services.

In these ways they 'outsource' much of their security needs to specialists. They increasingly *expect* that other cyber-services they deal with – such as retailing through Amazon or interacting with HMRC to make filings – will be secure services that they do not have to defend against.

It is important that SMEs understand their individual threat model, and take commensurate action. Many SMEs are unaware of the precise nature and extent of threats, and the consequences to their businesses.

The consumer market can (in terms of a supply side view) be viewed as a subset of the SME market, primarily buying products and services with security features bundled or simple tools from retailers and the Web. While the consumer market has a relatively high adoption of basic cyber security software such as anti-virus software, these are

[†] Using the ONS definition of firms employing 250 people or less.
[‡] We are acutely aware of the flaws in lumping all SMEs together or, worse, lumping SMEs with consumers. However, in the case of cyber security, there are sufficient similarities in supply chain characteristics to make the segmentation valid from a supply-side analysis perspective.

increasingly bundled with laptops, tablets and mobile devices. A key feature of the consumer market is ‘freeware,’ particularly firewall and antivirus software from Microsoft, AVG and others, severely limiting the revenue potential for specialist providers. Small businesses are also often happy to take advantage of these.

3.1.5 Segmenting the buyer needs

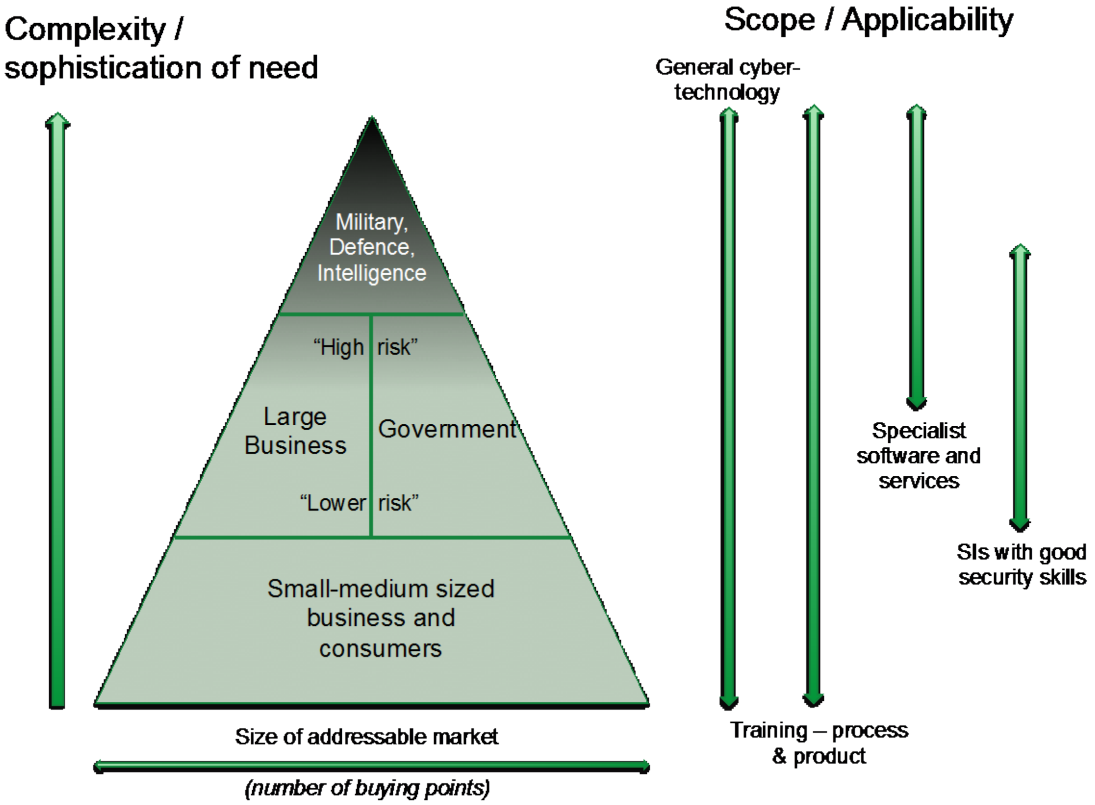

Complexity / sophistication of need
Scope / Applicability
General cyber-technology
Military, Defence, Intelligence
“High risk”
Large Business
Government
“Lower risk”
Small-medium sized business and consumers
Size of addressable market
(number of buying points)
Specialist software and services
SIs with good security skills
Training – process & product

Fig. 6: A hierarchy of needs

The four-market segmentation presented in the previous section describes the routes to market and is the basis for much of our analysis of the market’s operation. But as this section also highlighted, another useful view on these markets tells us how there is a *hierarchy of needs* in the market, which are satisfied in different ways: figure 6 depicts this graphically.

The highest level of need – the most complex and demanding requirements come from the defence/intelligence community, closely followed by certain segments of large business and Government – e.g. banks in the commercial sector (where financial gain is a big motivator for cyber-criminals), and high profile IT providers such as Amazon or Google. These will need – and be willing to pay for – solutions and advice from specialists. Thus the specialist contractors have a wider market than simply the defence industry.

Most of government and large business, however, has less stringent needs, which can often be satisfied by the large software providers, supplemented with services from large services providers. But still far stronger requirements than small-medium size business and consumers whose needs are generally met by volume products providers and non-specialist support services. There is thus a cascading effect and this deeply affects the buying points and addressable markets for providers.

So for example, a training service provider to a small business is likely to be a small generalist, possibly a value added reseller also offering SME-focused products, perhaps with a vendor-specific product certification (such as McAfee Certified Product Specialist). Security training for a large enterprise is likely to be a mid-sized specialist firm or a specialist practice of a large consultancy, certified to CISSP or perhaps CLAS level.

The key message from this is that solutions developed for organisations at the top of the hierarchy will be of decreasing applicability and interest to organisations in lower layers. Conversely, solutions developed for the lower levels may not be powerful enough or configurable enough for organisations at higher levels.

Skills and solutions for the defence industry may be of interest to banks, but general government and business organisations will find many of them too sophisticated for their needs, too complex and expensive to implement and use.

So, just as sales and marketing mechanisms must be changed if a provider wants to move from selling in one market segment to another (e.g. from large business sales to SME), then equally the nature of the solution offered is likely to need changing in terms of its power, usability and so forth. Skills and solutions are not transferable up and down the hierarchy simply because organisations have cyber security needs at all levels.

3.2 MARKET SEGMENTATION BY SECURITY SOLUTION TYPE

In Section 2 we mapped out some of the emerging technologies in the broad cyber security space. Such is the pace of change in technology – and threats – that it can prove difficult to define the market in technology terms. What is state-of-the-art one year will be commoditised the next. This can have a limiting effect on market growth and it is important for suppliers to build such commoditisation into their business models – or to try to avoid building their businesses around technology segments likely to be affected.

One way of viewing the market is to segment it by solution types, showing what is being protected by some combination of technologies – as depicted in Fig. 1.

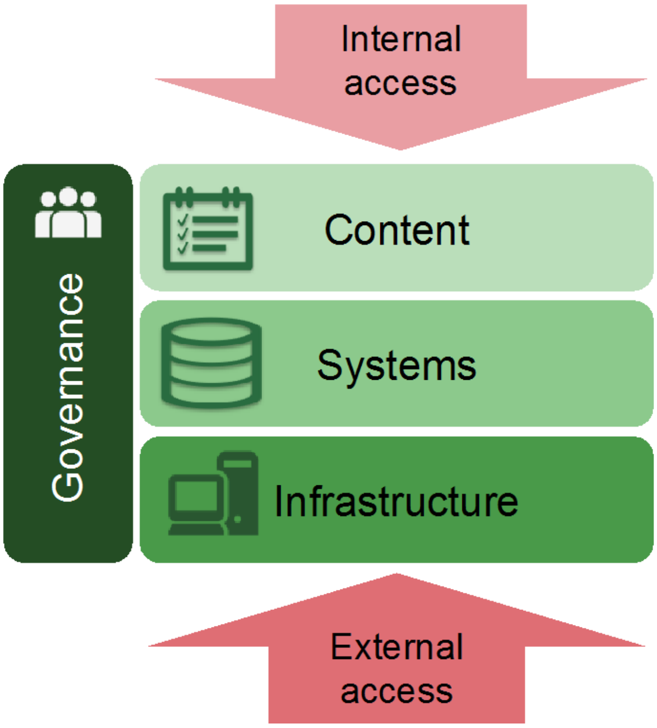


Fig. 7: **Understanding the market by solution type/buyer needs**

3.2.1 Infrastructure

Cyber security today is primarily based on infrastructure solutions, addressing both enterprise and personal IT security. This type of security deals with the access/entrance points to the systems, to offer a secure perimeter to the company IT. It includes network and device/end-point security.

This segment is largely based on anti-virus and firewalls. It also includes IPS, VPN, Secure Web Gateways, disk encryption, white listing, Unified Threat Management (UTM) that combines several of the solution mentioned above.

Those solutions are often implemented as appliances that include hardware device and software. These are rapidly becoming commoditised, but form the foundation of any type of cyber security. Excluding Defence and Homeland Security contractors, most of today’s leading cyber security specialists come from this segment.

3.2.2 System

This level of security deals with the protection of the organisations’ internal systems. If infrastructure security decides whether you can enter, then system security decides what you can do after you’ve entered. It includes all authentication mechanisms, directories management and provisioning software. This market is dominated by IT system management software vendors, and despite its maturity, it is still a dynamic market. It consists of three segments:

- Directory Services, such as Microsoft Active Directory
- Infrastructure Access Management/ID Management, where system management players dominate
- Critical Infrastructure Security Systems, where defence and homeland security players dominate.

System security began as a purely software segment, but the latest solutions are based on a combination of tightly coupled hardware, network and software systems. .

3.2.3 Content

This type of security deals with access to documents and applications. Encryption has been a key content security tool for many years and archiving also plays a role, but the other parts of this market are fairly new. It includes:

- Encryption, signatures, public key infrastructure (PKI)
- Digital Rights Management (DRM) and Information Rights Management (IRM)
- Data Loss Prevention (DLP)
- Secure by Design & Applications Security.

This software-based market is highly dynamic, and generates considerable IT services.

3.2.4 Governance

This is where security is managed, the conductor of the cyber security system. This part of the market is very intensive in services and has strong links with the other cyber security market segments. Governance consists of the following sub-segments:

- Cyber security strategy
- Risk Management
- Architecture
- Audit, Intrusion Tests & Post-Mortem
- Regulation & Certification Controls
- Recovery & Continuity Plans
- Security Incident & Event Management, (SIEM)
- Asset & Vulnerability management.

3.3 MARKET SIZE AND GROWTH IN THE UK

The cyber security market in the UK is worth almost £2.8 billion in 2013[§]. It is one of the most buoyant and fast-growing segments of the IT industry, and we estimate that the market will be worth over £3.4 billion in 2017, with a compound annual growth rate (CAGR) of 5.7%.

By comparison, the total IT market in the UK is set to more or less track inflation[5] and grow by only 2.1% CAGR to 2017[**].

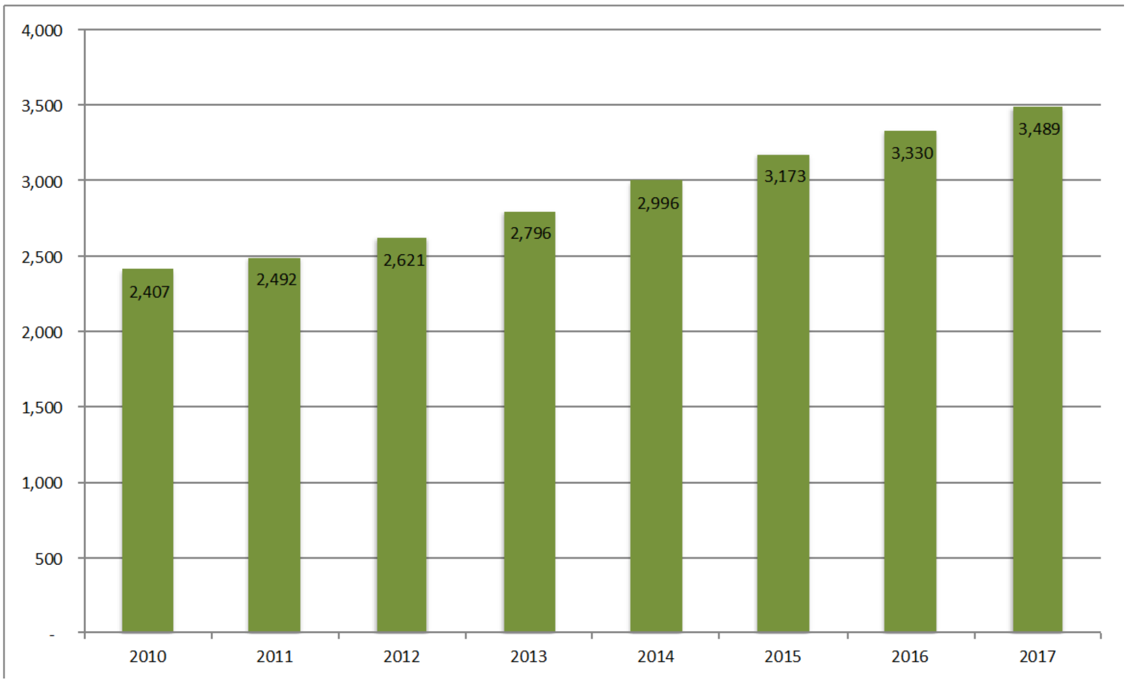


Fig. 8: UK Cyber security market size and growth 2010 – 2017 (£m)

3.3.1 Three types of market segmentation

Within the cyber security market, however, there is a wide difference of growth rates across the various technologies, uses and market segments.

To illustrate the complexity of the cyber security market, and to shed some light on the various sub-segments that are growing fast, we have provided three different views of the market figures:

[§] Our sizing and forecast methodology is provided in Appendix B

[**] Market numbers are nominal and are not adjusted for inflation. We assume inflation in the cyber security market is consistent with inflation of the overall UK economy.

- A segmentation of the market using our 'Four Market' model, showing separate market sizes for: Defence & Intelligence; other public sector; Private enterprises (over 500 employees); and SMEs and consumers.
- Market figures by solution type: infrastructure; systems; content; and governance
- A simple breakdown by IT product/service type, showing the market size for software and hardware, and for various types of services

These views show that, for example, cyber security infrastructure volumes, while still growing in absolute terms, are likely to be similar to the overall IT market. But spend on security governance will outstrip baseline IT market growth by growing at nearly 10% CAGR.

3.4 MARKET STRUCTURE BY SUBMARKET

Our preferred way to understand the market and its growth is in terms of the buyer segmentation we presented in section 3.1. As we explained earlier, success in one of these does not go very far in creating success in another. In particular, companies who are successful in the defence / military sector are fish in a relatively small pond.

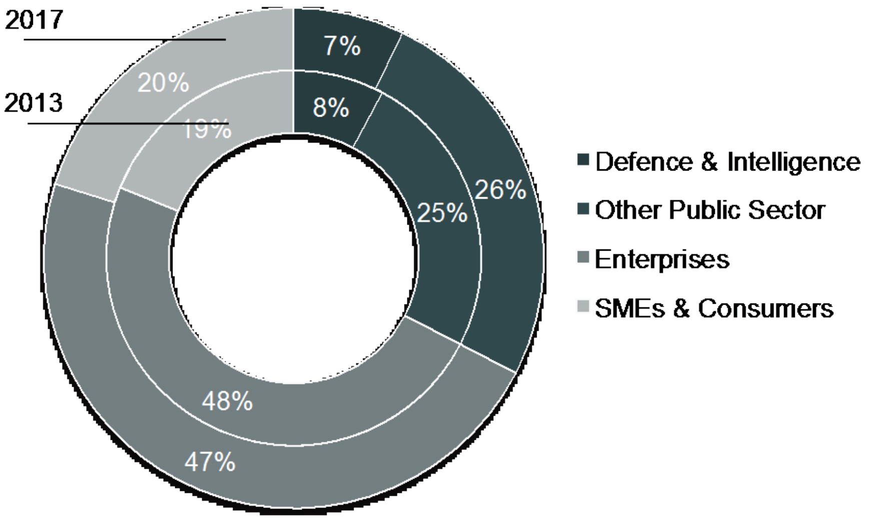


Fig. 9: **UK Cyber security market 2010 – 2017 by solution buyer type**

While it is a common perception that the majority of cyber security spend occurs within the public sector, our market figures show that this is not the case. In fact, private sector investment in cyber security is double that of public spend on cyber security.

And within the public sector, again the prevailing perception is that most spend occurs in the defence and intelligence space, whereas we estimate that this accounts for only one third of overall public sector spend on cyber security. This misperception is accounted for both by a general *overestimation* of the spend on cyber security from within the defence and intelligence sectors, and an *underestimation* of the spend within public sector segments such as health and local government. Although cyber security spend within defence and intelligence is higher relative to its overall spend on IT, it is very concentrated on specific agencies, the MOD and GCHQ in particular.

We predict that the markets for cyber security in defence and intelligence will increase at 3.4% CAGR, but the rest of the public sector is playing catch up, and will grow at a much higher 6.4%. In the private sector, large enterprises have a mature view of cyber security and its adoption is growing at an encouraging 5% CAGR. But we estimate that the greater potential for growth lies in the SME and consumer segment, and we predict a CAGR of 7.5% to 2017. This prediction is driven mainly by the large untapped addressable market in this sector, but it also assumes a higher growth in demand than we have seen to date. In this regard we take a positive view of the impact of interventions already taken by BIS, but we also assume that our recommendations provided in Section 7 are implemented and have a positive impact.

3.5 MARKET STRUCTURE BY SOLUTION TYPE

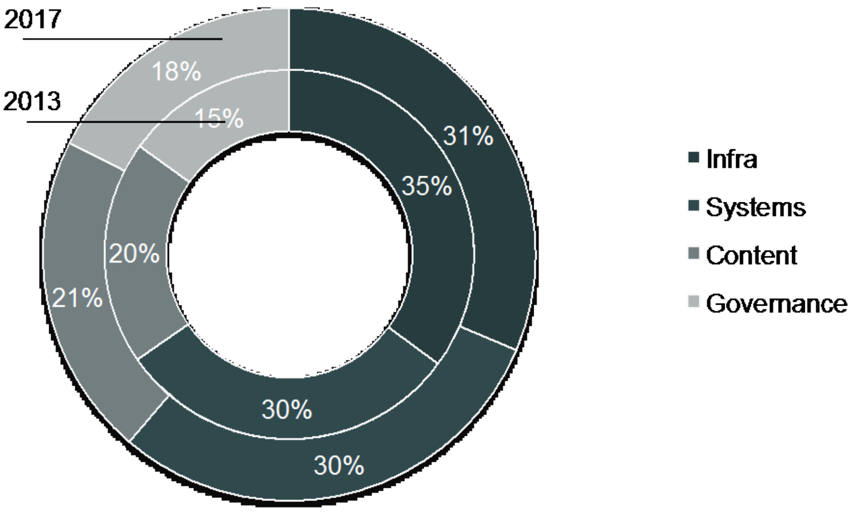


Fig. 10: **UK Cyber security market breakdown 2010 – 2017 by solution type**

Within the cyber security market, there is a wide difference of growth rates across the various technologies, uses and market segments. Using our segmentation by solution type, as presented in section 3.2, for example, cyber security *infrastructure* volumes, while still growing in absolute terms, are likely to see growth similar to the overall IT market. But spend on security *governance* will outstrip baseline IT market growth by growing at nearly 10% CAGR.

This is largely down to the maturing cyber security market. This is a natural progression of maturity, from infrastructure security, through systems and content security, to governance. Early implementations were based on infrastructure technologies, such as anti-virus software. As we said earlier, much of this technology is being commoditised, and so the value of the market grows more slowly (despite volumes potentially increasing).

Conversely, security technologies and services related to governance are growing strongly, albeit from a lower base, as they emerge to address key current issues such as complexity management and compliance.

3.6 MARKET STRUCTURE BY IT PRODUCT/SERVICE

We can also look at this market in terms of the vendors' solution service types – software, hardware, implementation and consulting services This shows us that spending on hardware is declining as a share of the market, growing at 3.2% CAGR, whereas services are growing at between 8% and 9% (depending on the type of service) – see Fig. 7.

Again, this demonstrates the maturity curve for security technologies. We see less investment in hardware and network equipment, due to commoditisation, and more spend being directed towards value-added services. Importantly, governance lends itself well to a service-led model, so as solution types mature this drives a further conversion from on-premise deployment of technology to fulfilment a service.

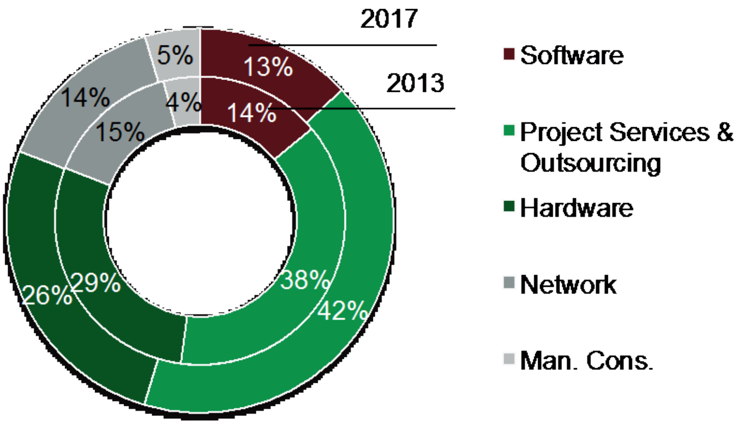
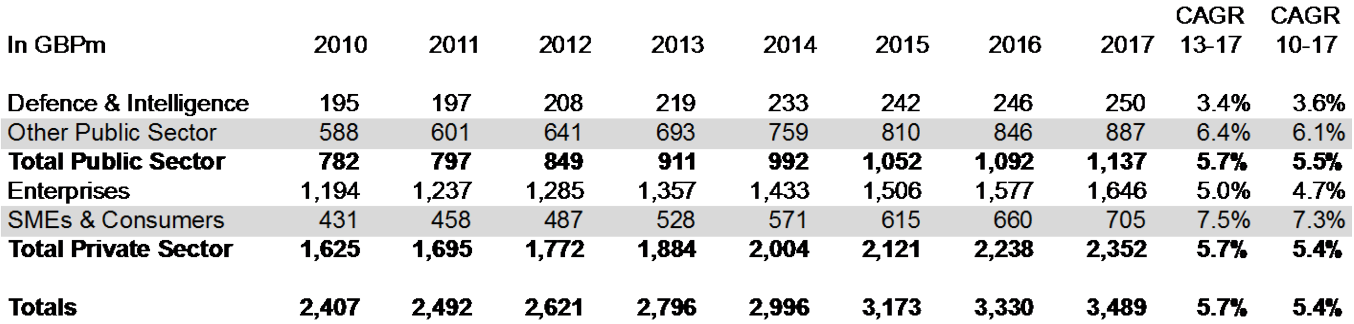


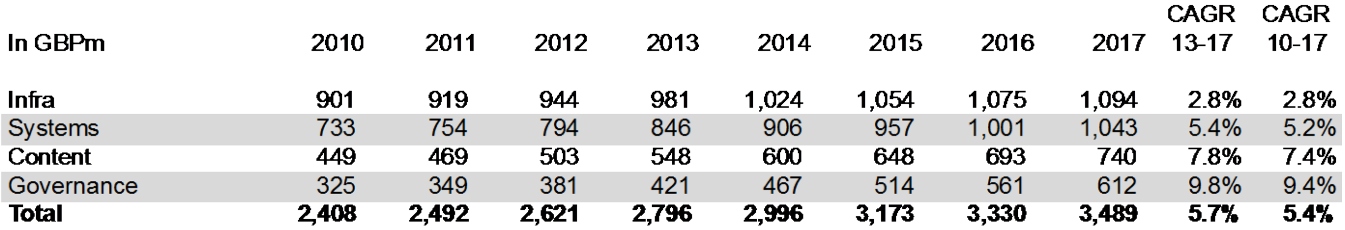
Fig. 11: **UK Cyber security market 2010 – 2017 by IT solution type**

3.7 UK MARKET FORECASTS IN TABULAR FORM



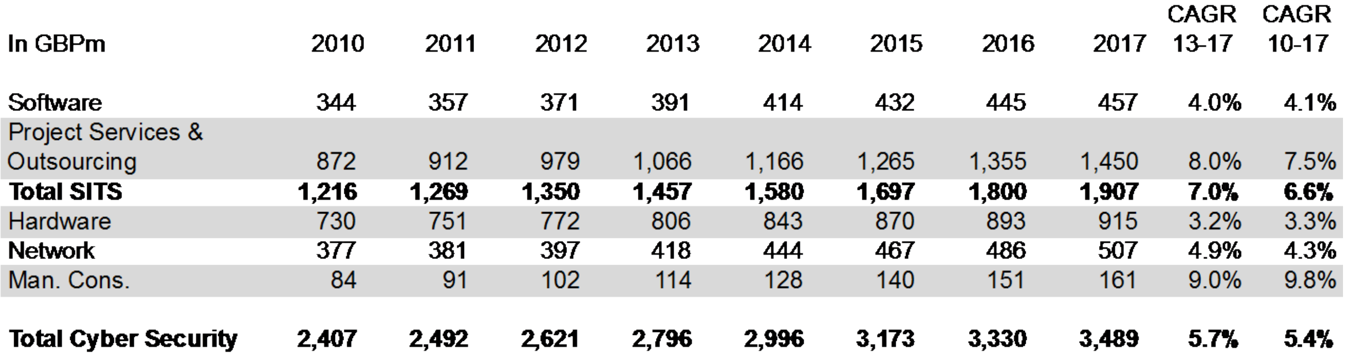
In GBPm	2010	2011	2012	2013	2014	2015	2016	2017	CAGR 13-17	CAGR 10-17
Defence & Intelligence	195	197	208	219	233	242	246	250	3.4%	3.6%
Other Public Sector	588	601	641	693	759	810	846	887	6.4%	6.1%
Total Public Sector	**782**	**797**	**849**	**911**	**992**	**1,052**	**1,092**	**1,137**	**5.7%**	**5.5%**
Enterprises	1,194	1,237	1,285	1,357	1,433	1,506	1,577	1,646	5.0%	4.7%
SMEs & Consumers	431	458	487	528	571	615	660	705	7.5%	7.3%
Total Private Sector	**1,625**	**1,695**	**1,772**	**1,884**	**2,004**	**2,121**	**2,238**	**2,352**	**5.7%**	**5.4%**
Totals	**2,407**	**2,492**	**2,621**	**2,796**	**2,996**	**3,173**	**3,330**	**3,489**	**5.7%**	**5.4%**

Fig. 12: **Cyber security market size 2010 – 2017 by buyer/market segment (£m)**



In GBPm	2010	2011	2012	2013	2014	2015	2016	2017	CAGR 13-17	CAGR 10-17
Infra	901	919	944	981	1,024	1,054	1,075	1,094	2.8%	2.8%
Systems	733	754	794	846	906	957	1,001	1,043	5.4%	5.2%
Content	449	469	503	548	600	648	693	740	7.8%	7.4%
Governance	325	349	381	421	467	514	561	612	9.8%	9.4%
Total	**2,408**	**2,492**	**2,621**	**2,796**	**2,996**	**3,173**	**3,330**	**3,489**	**5.7%**	**5.4%**

Fig. 13: **Cyber security market size 2010 – 2017 by solution type/need (£m)**



In GBPm	2010	2011	2012	2013	2014	2015	2016	2017	CAGR 13-17	CAGR 10-17
Software	344	357	371	391	414	432	445	457	4.0%	4.1%
Project Services & Outsourcing	872	912	979	1,066	1,166	1,265	1,355	1,450	8.0%	7.5%
Total SITS	**1,216**	**1,269**	**1,350**	**1,457**	**1,580**	**1,697**	**1,800**	**1,907**	**7.0%**	**6.6%**
Hardware	730	751	772	806	843	870	893	915	3.2%	3.3%
Network	377	381	397	418	444	467	486	507	4.9%	4.3%
Man. Cons.	84	91	102	114	128	140	151	161	9.0%	9.8%
Total Cyber Security	**2,407**	**2,492**	**2,621**	**2,796**	**2,996**	**3,173**	**3,330**	**3,489**	**5.7%**	**5.4%**

Fig. 14: **Cyber security market size 2010 – 2017 by IT product/service (£m)**

4. Market potential

4.1 EXPORT POTENTIAL

The export market is already very important for UK cyber security products and services suppliers. Exports account for around 20% of the total UK cyber security market[6].

Of the 600 UK-headquartered organisations covered in our analysis, more than 60% already sell to clients based outside the country. All of the UK's ten largest cyber security companies have developed or acquired substantial overseas businesses, with the best-known examples being QinetiQ and BAE Systems.

BAE Systems has built a strong US cyber security business and recently opened a new security operations centre (SOC) in the country and ended 2012 with a North American order pipeline of cyber security related business of £1.8bn. It is also in the process of adding more than 50 new consultants to its 200-strong workforce in the Asia Pacific region.

But it is not just the large suppliers that have set their sights on international markets. For example, Titania, a Worcester-based supplier of cyber security auditing software makes over 80% of its revenue from outside of the UK. Cambridge Intelligence, a start-up company that develops a network visualisation product called Keylines, has recently opened its first US office in order to tap into interest from both government and private sector clients. However these small companies are often reliant on in-bound queries from overseas and have little cash to market themselves on an international stage in a manner to match large overseas suppliers.

It is not just products companies that are benefiting from exposure to international markets. Mid-size consulting and penetration testing firm Context Information Security has established direct sales and delivery operations in Germany and Australia in order to support global clients in sectors such as financial services, retail and professional services.

NCC Group, a Manchester-based provider of escrow and assurance services, expanded the international footprint of its security testing business with the £7.1m acquisition of New York-based Intrepidus Group. The deal was NCC's third takeover in the US, which helped it grow its security testing business by 51% in fiscal 2012.

Exports are particularly important for those UK cyber security suppliers selling to the "high risk" of Fig. 6:. These can often use their relationships with UK defence and intelligence as a springboard to business with overseas bodies. Based on our discussions with UK cyber security suppliers, it is clear that credentials administered by CESG carry a lot of weight with defence, intelligence and government bodies, notably in the US, Middle East and Australia.

Also, for true specialists, the buyers will actually seek them out based on word- of-mouth or Internet search. But for those selling more general solutions and targeting general users and government, good sales and marketing stratagems and knowledge are essential if they are to grow their business overseas. Assistance with market identification and sizing, competitor and prospect identification e.g. from Government could be vital external services to unlock that potential for the smaller firms in the market.

However, it will be equally crucial for technology and services providers targeting large commercial sector organisations that they are able to extend their reach into international markets, because many of the key players in the UK manufacturing, pharmaceutical, banking are based in the US and Europe and will first look to their home markets when they are putting their security standards and strategies in place.

4.2 INVESTMENT POTENTIAL

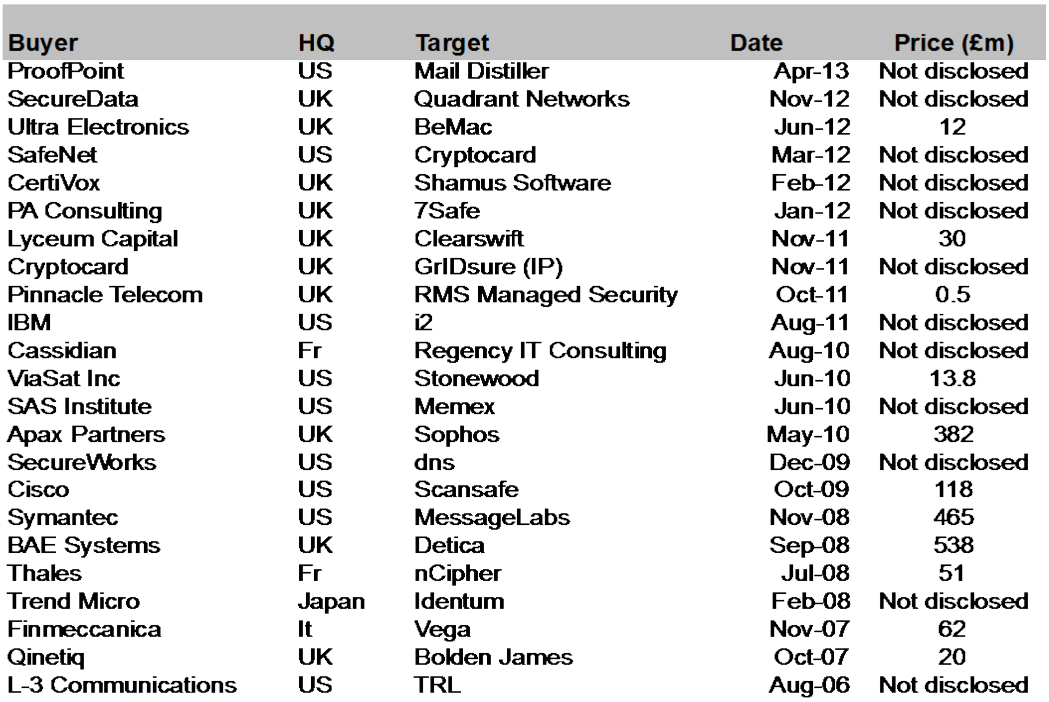
Although our analysis indicates a buoyant and healthily growing market for cyber security products at home and abroad, it does not automatically follow that the UK cyber security industry will be able to capitalise on this situation.

4.2.1 Can the UK produce global champions?

As we discuss in the Supplier Landscape section (Section 2.4), very few UK cyber security business have been able to grow the business to a critical mass where they can stand as genuine international players in their respective fields. On the services side, there is BAE Systems Detica and QinetiQ, while Sophos is the sole UK-headquartered cyber security software player whose annual sales exceed £100m.

One of the main reasons is that M&A remains the preferred exit route for UK technology companies. In Fig. 15:, we provide an overview of notable acquisitions of UK-headquartered cyber security companies. Two things are very clear from this. First, that the acquiring companies are from outside the UK in over half the cases. One UK acquirer, Cryptocard, was itself acquired by a US company less than six months later. And, second, that most of the acquired companies were snapped up before they reached a significant size (beyond the SME classification of 250 employees).

There are a number of reasons for this, few of which are unique to the cyber security industry. This question is part of a debate that has long raged in the wider UK's technology sector and investment community, as to why the country has produced so few companies that have been able to stand on a global stage against the cream of Silicon Valley.



Buyer	HQ	Target	Date	Price (£m)
ProofPoint	US	Mail Distiller	Apr-13	Not disclosed
SecureData	UK	Quadrant Networks	Nov-12	Not disclosed
Ultra Electronics	UK	BeMac	Jun-12	12
SafeNet	US	Cryptocard	Mar-12	Not disclosed
CertiVox	UK	Shamus Software	Feb-12	Not disclosed
PA Consulting	UK	7Safe	Jan-12	Not disclosed
Lyceum Capital	UK	Clearswift	Nov-11	30
Cryptocard	UK	GrIDsure (IP)	Nov-11	Not disclosed
Pinnacle Telecom	UK	RMS Managed Security	Oct-11	0.5
IBM	US	i2	Aug-11	Not disclosed
Cassidian	Fr	Regency IT Consulting	Aug-10	Not disclosed
ViaSat Inc	US	Stonewood	Jun-10	13.8
SAS Institute	US	Memex	Jun-10	Not disclosed
Apax Partners	UK	Sophos	May-10	382
SecureWorks	US	dns	Dec-09	Not disclosed
Cisco	US	Scansafe	Oct-09	118
Symantec	US	MessageLabs	Nov-08	465
BAE Systems	UK	Detica	Sep-08	538
Thales	Fr	nCipher	Jul-08	51
Trend Micro	Japan	Identum	Feb-08	Not disclosed
Finmeccanica	It	Vega	Nov-07	62
Qinetiq	UK	Bolden James	Oct-07	20
L-3 Communications	US	TRL	Aug-06	Not disclosed

Where terms are "not disclosed" the acquired company is generally an SME

Fig. 15: **Notable acquisitions of UK cyber security companies**

General factors militating against growth to large scale include:

- *Access to funding for growth is easier in other countries.* PAC research established that there is a widespread consensus while angel and seed funding is quite widely available in the UK, VC-style 'venture funding' at the mezzanine level sufficient to build companies to larger scale is less in evidence. Smaller firms interviewed by PAC reported that many of the approaches come from US-based venture funds. Meanwhile, with a few exceptions, UK-based PE firms are on the hunt for companies with established profit and growth track records. According to E&Y (based on Dow Jones)[7], "*the US maintains a strong lead, with about 70% of global investment in any given year"* with $33bn of investments in 2011, compared to $6.1bn across the whole of Europe (including the UK).

- *Valuations of tech companies are higher in other countries, particularly the US.* This makes it easy for a US-quoted company to pick up a UK company and instantly show value.

- *UK companies are often very wary of venture capitalists.* In interviews, companies told us "they want rights to everything up to my first-born child"… "they are a great source of funds but you really have to understand what you're getting into."

- *Bank lending is currently very hard to come by.* After the banking crisis of the late 2000s, this source of funding has all-but-dried up for smaller companies of most types. Yet small businesses are the mainstay of the UK cyber security sector. Cyber companies reported that they have to give too-solid guarantees and that their businesses are just not stable or certain enough for banks who are trying to reduce risk in their lending. Thus they are having to run on capital raised from current operations, which doesn't allow them to quickly grow.

- *The UK stock market is a mixed blessing for smaller companies.* Some companies we interviewed think that moving onto AIM is good move, as there are few tech companies and so this gives great visibility amongst investors. *"On NASDAQ you need a $1bn turnover before anyone notices you."* Others however feel that AIM gives exposure to the few investors who are interested in the fairly risky nature of a cyber security supplier investment.

- *Many SMEs lack the knowledge of international markets they need to operate effectively overseas.* Some have exported very successfully but even those who are exporting successfully would welcome better intelligence on countries, opportunities and competitors overseas. However this information can be hard (or expensive) to acquire. Meantime particular niches in the domestic market are relatively small. US firms in particular have a much wider domestic market to target before they need to think about international expansion.

- *SMEs don't have the resources to monitor the developments in their big competitors.* One major UK technology services supplier – one of the biggest cyber security vendors – said that they are approached by at least one small cyber security start-up on a monthly basis interested in a partnership/alliance. However, the biggest problem that they identified in their propositions is that they don't have sufficient competitive intelligence to understand where their product sits in the market. In one case, a company was pitching a proposition of which 80% would be covered by a forthcoming update of Cisco's Internetwork Operating System (IOS).

- *Experience of management/industry knowledge is often the missing ingredient.* Many of those running smaller cyber security businesses – in common with other small UK tech companies – are experienced in their technical domain, which is how they establish their business. But they are lacking in more general commercial knowledge – how to grow a business, how to deal with VCs, how to identify prospects in new markets segment, how to prepare for an IPO.

Cyber-security-specific factors include:

- *The size of the cyber security market* in many areas outside basic anti-malware tools is not particularly large (relative to, say, cloud or mobile IT) and more important are populated by large companies with well-established channels and customer bases. It's often easier for them to acquire promising startups than for the startups to find new customers.

- *The start-up and on-going costs for a cyber security company* can be higher than for other technology businesses. Cyber security can require high equipment costs up-front, and those we spoke to cited a high cost of sale and difficulty in proving credentials to secure early success. The cost of gaining CESG accreditation in order to establish credibility for their products or services is high for a small business. For example, to be assessed as a CHECK rated supplier of testing services incurs an annual cost of £7,500. SMBs find this prohibitive, or at least unfair, as the flat fee does not reflect level of revenues. This inhibits them from growing or launching new offerings.

- *Security products also require a rigorous testing stage*, often incorporating a broad range of devices and networks and undertaken by experienced and skilled penetration testers. The use of cloud-based platforms can alleviate some of the cost for test and development, but for high-end cyber security products, this may not be an option.

- *The cost of sale is often high* for those companies looking to operate in the defence and intelligence markets, and often requires them to develop relationships with larger consultancies or systems integrators in order to gain access to target accounts. Sales cycles can be lengthy and payment spread out over long periods, which applies huge pressure on cash flow.

4.2.2 Still attractive for venture funding – particularly products

Nonetheless, the investment community regards cyber security as one of the more attractive areas of the UK technology sector, based on growth potential and the indigenous skills base. For them, the idea that the most likely exit is trade sale to an overseas buyer is not an issue.

Recent examples include secure e-mail provider Mimecast securing £40m from Insight Venture Partners, and Clearswift receiving £30m from Lyceum. In 2010, Apax Partners invested some £380m to acquire a 70% stake in Sophos, which had drawn back from an IPO.

Despite the issues discussed in the previous section, there remain good short and longer-term growth prospects for UK-based cyber security services companies.

As discussed elsewhere in this report, this is a fast-evolving area and new techniques are constantly required and being devised as a response to ongoing efforts of those trying to break government and business security defences.

The scarcity of cyber security skills means that those companies that are able to recruit and retain the best people, either through fostering close links with academia or through brand development, will be in demand.

In the era of cloud-based delivery, it is much easier for a security software vendor to reach an international audience. For example, cloud-based security, mail and archiving specialist Mimecast has grown its business over the last five years by more than

1,000%, and has established a client base of 6,000 customers and 1.6 million users worldwide.

Prominent venture capital groups in the UK technology sector, Amadeus and Notion Capital, both believe that the most attractive investment opportunities sit in cyber security products companies, rather than professional services organisations.

This is because people-based businesses are more difficult to scale. There is a linear relationship between the growth of the business and investment in headcount, and retaining and recruiting the right skills is challenging in a market with relatively scarce resources such as cyber security. There is also strong competition for talent from larger companies such as Deloitte, KPMG, QinetiQ and IBM.

PAC also believes that while the domestic UK IT services supplier community has been negatively impacted by strong pricing competition from offshore (largely Indian) vendors, cyber security will not be affected to the same extent. While some network monitoring and secure systems development and maintenance work is already being delivered from low-cost sourcing locations, the majority of the advisory, compliance consulting and systems integration will by its nature have to be delivered by onshore teams. While this mitigates the threat to domestic work by domestic companies it also implies that services companies wishing to export their skills will need staff prepared to work on-site on overseas locations or establish subsidiaries in key countries.

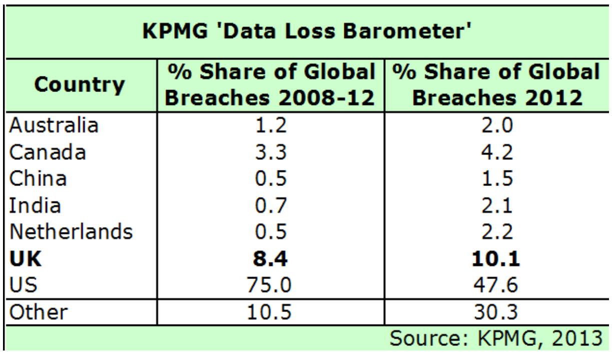
Consolidation is inevitable in such a fragmented supplier market. We expect a wave of M&A activity among the smaller services companies as they look to make the jump from being local to regional or national players. And as they develop their relationships with customers, they will also seek to extend both their scale and portfolio in order to take on broader engagements.

5. International comparison

5.1 THE GROWING CYBER THREAT IS WIDELY RECOGNISED

The number of nations drafting and launching National Cyber Security Strategies (NCSSs) in order to formalise their position on and response to cyber threats demonstrates that cyber security is a critical concern for nation states.

Significantly for the UK, international data breach studies suggest that it is the second largest source of data breaches after the US, and its share of global data breaches is growing. For example as shown in the table below, this trend is demonstrated by KPMG's 'Data Loss Barometer'[8], which compares the share by country of global data breaches in 2012 with the share by country over the 2008-12 period:



KPMG 'Data Loss Barometer'

Country	% Share of Global Breaches 2008-12	% Share of Global Breaches 2012
Australia	1.2	2.0
Canada	3.3	4.2
China	0.5	1.5
India	0.7	2.1
Netherlands	0.5	2.2
UK	**8.4**	**10.1**
US	75.0	47.6
Other	10.5	30.3

Source: KPMG, 2013

Fig. 16: **KPMG 'Data Loss Barometer' 2012 - extract**

While the US share of data breaches has declined significantly, the rest of the world has become a much greater target. Also, despite the US *share* of total breaches falling, this amounts more to a 'smaller slice of a bigger pie' rather than a declining threat in absolute terms.

In the KPMG study, the UK is considerably higher than its peers. Germany's share of breaches 2008-2012 is 0.5%, despite it having a similar profile of Internet adoption and regulation.

With cyber threats growing in both frequency and impact, it is clear that NCSS responses need to evolve. Nations such as Japan, the UK and the US can point to the launch of multiple NCSS iterations, responding to the evolving nature of cyber threats. While this is a positive sign, it also highlights one of the systemic challenges of cyber security: while cyber threats operate within a fluid environment, NCSSs by their very nature are fixed, being updated periodically.

5.2 QUANTITATIVE INTERNATIONAL COMPARISONS

5.2.1 Introduction

In order to provide an indication of the UK’s cyber security maturity compared to its international peers, PAC has conducted comparisons based on IT security market expenditure by country. Note that this *market volume* data, relating to external expenditure by organisations on products and services, and does not include organisations’ internal spending on IT staff salaries etc.

In PAC’s definition, IT security expenditure as presented below consists of software products, project services and outsourcing expenditure related to cyber security. Although this does not represent the full cyber security market volume, it does represent a significant proportion and so offers guidance.

5.2.2 IT security vs total software and IT services spend (2012)

To provide an indication of the ‘centres of gravity’ in the global IT security market, and the UK’s position related to that, PAC has compared countries on the basis of the share of the global IT security market that they represent against the share that IT security represents of in-country total software and IT services (SITS) spend. Our view is that countries that have a higher share of the IT security market will have a higher proportion of overall IT spend directed towards cyber security.

PAC concludes that there are currently three key zones within the global IT security market. First, there are the global centres of gravity, represented by the US and to a lesser extent Japan, that dominate the global IT security market in terms of volume, and therefore the share of the global market that they represent.

Within the second zone, the UK stands alongside Western European peers such as Germany (which is of a very similar scale to the UK) and France, as well as developed nations such as Australia and Canada. This shows that after the US and Japan, Germany and the UK jostle for leadership of this ‘chasing pack’ in terms of market size, while France is ahead in terms of how ‘security geared‘ its market is in terms of the share that IT security represents of its total SITS market.

Not far behind are the developing economies of Brazil Russia, India and China (BRIC). These countries are notable in that, despite having large and booming economies, they only represent a small share of the global IT security market, on a par with small Western European nations such as Finland and the Netherlands. This demonstrates the immaturity of IT security in the BRIC countries.

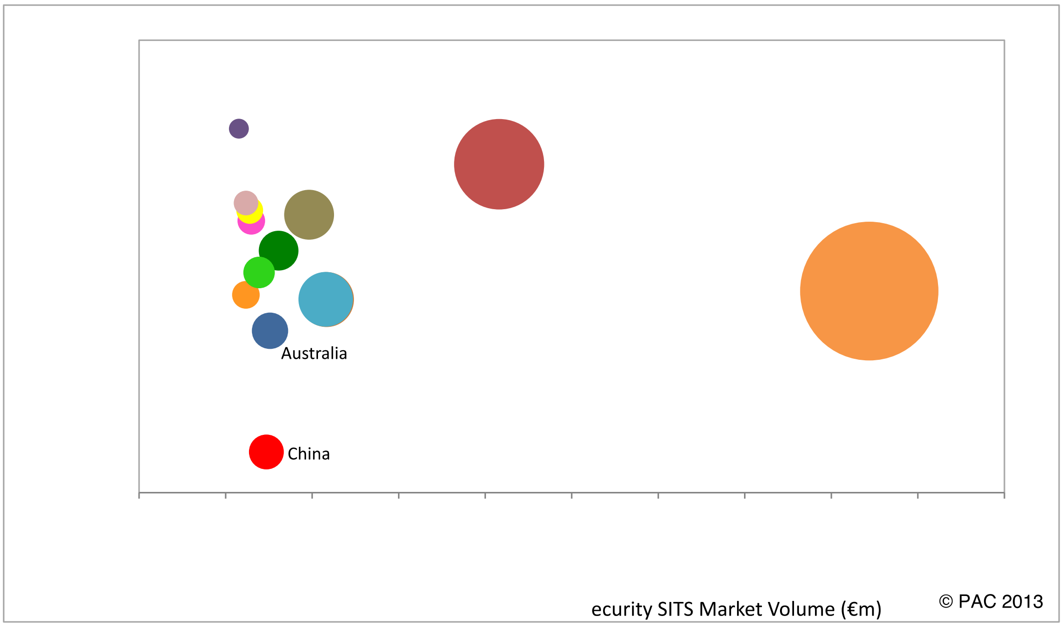


Fig. 17: **2012 IT Security Spend Proportion by Geography**

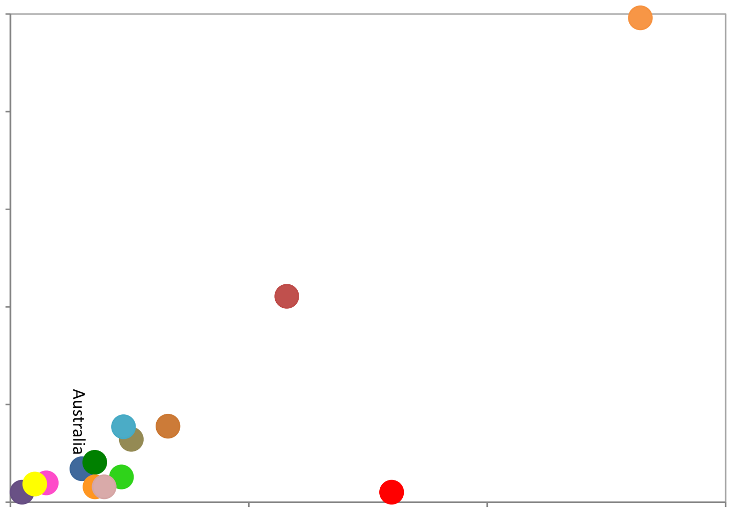
There are some significant outliers in this comparison. The first is the US, where, despite it accounting for such a large share of the global IT security market, only spends a middling proportion of its in-country SITS expenditure on IT security. This can be explained by the scale and variety of the US SITS market, which is among the most mature in the world. Yet this is not to downplay the US's military spending, which is by far the largest in the world and accounts for much of the US IT security market.

Another significant outlier is Finland. Although only representing a small share of the global IT security market, IT security represents the highest share of total SITS among the countries analysed. This shows the premium that is placed on IT security in Finland, particularly following the broad cyber-attack on neighbouring Estonia, which was observed closely by Finland and even impacted on some Finnish systems. Finland has reacted with one of the broadest NCSSs in terms of scope and the level of state control. However, this approach is much easier to implement in a comparatively small nation (in terms of population and economy) such as Finland, where for example critical national infrastructure can be centralised to a greater degree.

Russia's IT security market is similar to Sweden and the Netherlands in terms of size and share of total national SITS. However, while the latter are developed economies, Russia is more of a developing nation. This means that its share of total SITS that IT security represents is surprisingly high when compared to peers such as Brazil, India and particularly China. To an extent this is a result of, like the US, proportionately high military expenditure, which in turn drives IT security spend. However, PAC also believes that this can be explained by the nature of the Russian market itself, as protection against concerns such as corruption and organised crime that are arguably less widespread (although not insignificant) in Western European nations.

Finally, there is China where IT security spend has a very low share of total SITS, especially for a nation whose IT security market is of comparable size to Australia and Canada, and whose economy is far larger than both. In part this is explained by China's low costs, but also by the low level of maturity within the Chinese IT market overall, let alone IT security.

5.2.3 IT security spend compared to GDP



tion sourced from IMF

Fig. 18: **2012 IT Security Spend Compared to GDP (€m)**

A major concern for nations in plotting their approach to cyber security is ensuring that IT security spend keeps pace with economic growth. To provide an indication of the extent to which countries are achieving this, PAC has used IMF data[9] to compare IT security spend with GDP.

Our hypothesis here was that countries with larger economies will spend a greater amount on IT security.

Fig. 18:demonstrates that while most countries more or less adhere to the overall trend line, there are some outliers. As with the previous graph, the US and Japan are key examples, with IT security spend far outstripping the overall trend. While the US's IT security market may be slightly lower than average compared with the global IT security market from Fig. 17:, it is very strong in comparison with its GDP. The US's defence spending accounts for a large proportion of this strength.

At the other end of the scale, again China 'underperforms' when comparing IT security with GDP. This is even compared with its 'BRICS' peers, whose IT security spend outstrips China despite having far smaller economies. However, it is notable that IT security spend is lower compared to GDP in developing economies than more developed nations such as France, Germany and especially Japan and the US.

The UK is an outlier, particularly when compared with its Western European neighbours. While the UK was similar to Germany and slightly behind France in the previous comparison, here it is ahead of both. This suggests that the UK is spending more on IT security in order to protect its economy than its immediate, similar-sized neighbours. It also points to the UK's high military spend, particularly in comparison with Germany, although to a much lesser extent in comparison with France.

Another view of this data is given in Fig. 19:, which shows the same data, but this time with IT Security spend expressed as a proportion of GDP. It demonstrates that as a proportion of GDP the US is behind Finland, Japan and Sweden, with the UK just behind the US.

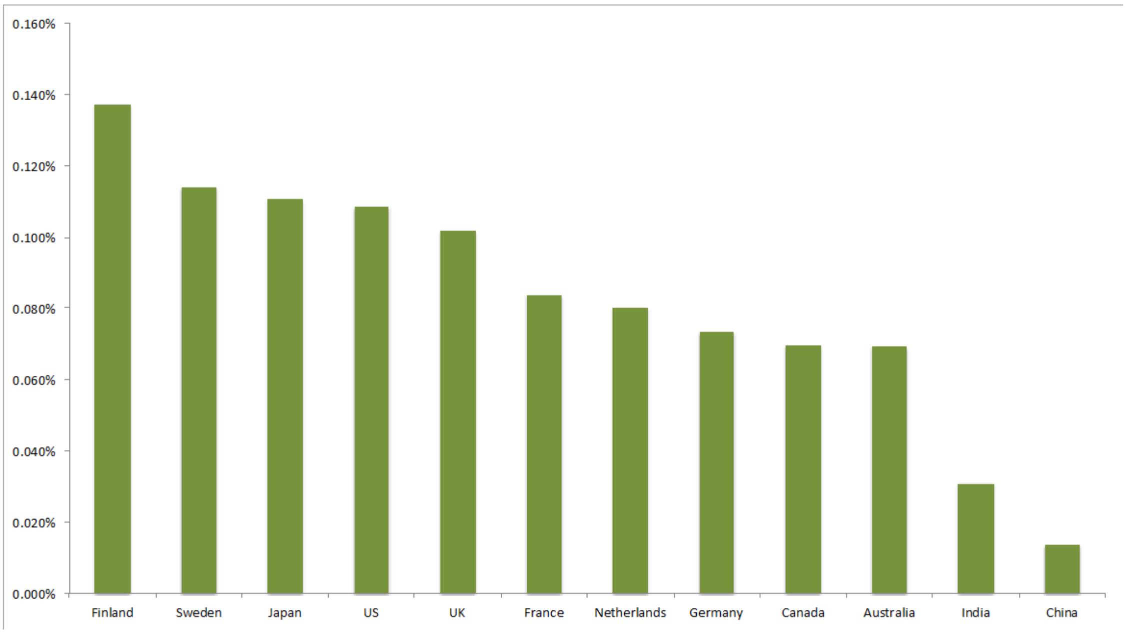


Fig. 19: **2012 IT Security Spend as a proportion of GDP (%)**

With section 5.1 of this report showing that the UK is a far larger source of data breaches than its peers, it is perhaps a natural step that a greater investment ought to be made in security. This is particularly the case when, as reported by the Boston Group in its '$4.2 Trillion Opportunity' report[10] of 2012, the UK's internet economy represents a higher share of GDP than any other G20 country.

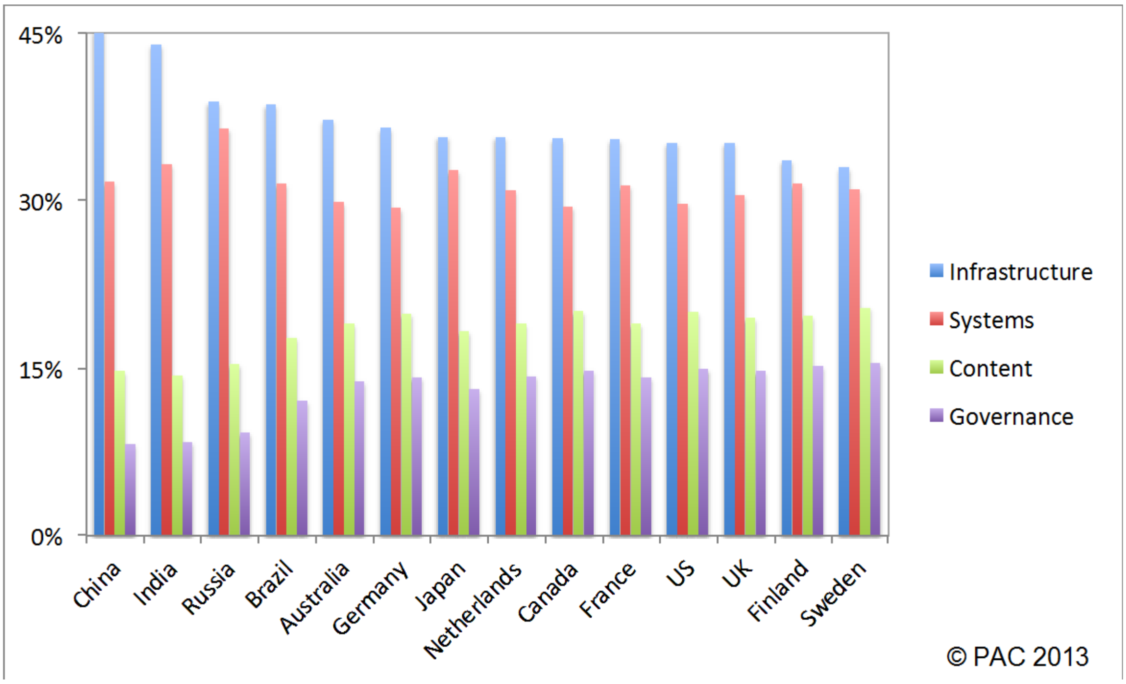
A challenge to this position is that, despite a higher spend on IT security compared to GDP, the UK still suffers a far higher level of global data breaches than the likes of France and Germany. However, language is a mitigating factor. Widespread use of the English language means that the UK represents a far easier 'secondary target' than non-English speaking countries. Similarly, countries such as Australia and Canada represent a higher share of global data breaches relative to their economies than countries such as China, India or Japan.

5.2.4 IT security spend by sub-segments

A measure of maturity in approach to cyber security that PAC's market figures can offer insight into is the' balance of market volume across sub-segments. The general rule is that more mature markets for IT security spend comparatively less on infrastructure and systems, and comparatively more on governance and content. For less mature markets, the balance is reversed.

This position is borne out by PAC's market figures, as shown in Fig. 20: below. For example, while developing countries such as China and India spend proportionately far more on infrastructure than developed nations such as Finland and the UK. This demonstrates the maturity scale of IT security sub-segments, with infrastructure being an initial focus, before moving onto more mature areas such as social media interpretation, which would fall within content.

Meanwhile, the opposite is true of governance, where more mature nations such as Sweden and the US spend a larger share of their overall IT security market on areas such as automated security management than countries with a less mature approach to IT security, such as Brazil and Russia. Against this benchmark of sub-segmental balance, the UK ranks alongside more mature markets such as Japan and the US.



© PAC 2013

Fig. 20: **Share of sub-segments within total IT security spend (2012)**

6. SWOT analysis

Summarising the above chapters enables us to present the following SWOT (Strengths-Weakness-Opportunities-Threats) analysis for the UK cyber security industry, taking into account its own capabilities, the UK market situation, overseas markets potential, and the competitive situation within the UK and of overseas cyber security technology and services providers.

6.1 STRENGTHS

6.1.1 The UK has world-class knowledge and companies

The UK has large defence contractors working globally on cyber security projects, including BAE Systems Detica and QinetiQ, and a CNI core competence at BT, together with specialist solutions suppliers and consultants, such as KPMG, who are sought after from around the world.

It also has a pool of UK talent in this area working for foreign-owned firms in the UK and overseas, including IBM, Deloitte, HP, Lockheed Martin, and CGI.

6.1.2 Large domestic market – with financial leverage

The UK is the fifth largest market for IT worldwide and the world's 6th largest economy. Relative to its economy, defence accounts for a high proportion of GNP.

Furthermore, the UK's financial services sector – which is a big spender on cyber Security solutions – is the third largest in the world. Some of the world's largest financial services organisations are headquartered in the UK or have key decision-makers located in the country. This presents an opportunity for UK cyber security companies to gain access to the accounts at the highest possible level and develop worldwide relationships.

All this adds up to a very significant domestic market, albeit currently much of that spending is currently with overseas companies, mainly from the US.

> "The UK offers global companies a vibrant marketplace to operate in and has the right combination of cyber security policy and governance, and technical and industrial expertise. It is aiming to foster a robust partnership with the private sector, a key requirement in order to improve cyber , reduce vulnerabilities and enhance the security posture of UK plc."
>
> **Ilias Chantzos, Symantec**

6.1.3 GCHQ is an international star with a global brand and pedigree

Cyber security is a well-established area of the UK technology industry, with GCHQ having been a key driver for the development of important process standards for well over a decade. Approval from GCHQ gives considerable merit to recipient companies in the military/defence/intelligence world in particular.

6.1.4 UK university R&D is world class

UK universities have some of the most respected research and cyber security courses in the world and are fostering close ties to the vendor community to help graduates into work. The centres of excellence initiative is a trend setter.

6.1.5 UK Aerospace & Defence industry is an asset

The UK is very strong in conventional security & defence sales around the world, in the top 5 defence exporters worldwide. This can have a ‘halo’ effect in making clients of UK defence firms favourably disposed toward products and services from UK-based cyber security suppliers. More directly, the same firm or its partners or associates can pick up cyber security work linked to that conventional security work.

Interestingly, although the UK has a leadership position in financial services this does not translate to a specific competence in related cyber security. We think this is perhaps because financial services security aspects are ‘evened out’ across the globe, due to international standards (such as PCI DSS).

6.1.6 Good public/private co-operation

The UK rates as above average in international comparisons in its relationships between public and private organisations. The Cyber Growth Partnership and the Cyber Security Information Sharing Partnership are instantiations of this. Other information sharing partnerships such as those set up by CPNI have been running for over 10 years.

6.2 WEAKNESSES

6.2.1 Talent pool and supplier community is limited in size/number

“Skills development is a major challenge. The Government is encouraging people into apprenticeships; in addition we should all recognise the importance of undergraduate courses. In a knowledge led economy we need design engineers as well as technicians.”

Richard Nethercott, CGI

The UK has a limited supply of qualified cyber security skilled personnel, and the strongly growing market means that the size and growth of the talent pool is a constraint on growth. There is a widespread sense within the small business supplier community that the number of accredited people is being kept low, with a commensurate inflation in salary market rates. As an indicator, CESG currently has 690 CLAS certified consultants listed on its website[††]. (Contrast this with over 150,000 chartered accountants.)

The talent pool issue is complicated. There are well-known concerns regarding school- and university-aged students studying STEM subjects. But employers are also concerned that STEM syllabuses don't prepare young people for entering the market. And small business employers state that training employees in cyber security is

[††] As of July 24th, 2013.

expensive, and exposes them to the risk of training young professionals only for them to leave for higher salaries at larger firms.

6.2.2 Limited links between business and academia

Large enterprises and government are aware of what’s happening in academia, and ready to exploit it, but SMEs (which arguably could benefit more from ideas and IP from academia) generally only see universities as a source of raw talent.

Some of our interviewees commented that universities are not aligned with business needs. Computer science syllabuses with insufficient security emphasis were cited as examples, and three-year PhD were considered too slow to produce solutions to business problems.

There are mixed views on the various TSB initiatives and their success to date. However, there is broad consensus that the TSB’s focus on cyber security is a good thing, and should continue.

The Cyber Challenge is universally endorsed as a means of promoting cyber security in the education sector.

6.2.3 Many suppliers lack scale, know-how & funding

Most of the UK’s indigenous cyber security suppliers are small scale. They find it hard to find funds to grow and they don’t have the resources or skills to grow business faster. Much of their sales are through word of mouth or by promoting themselves via the Internet and waiting for others to find them. This also affects R&D – where funds are limited then so is product development.

Many SMEs in the cyber security sector are very wary of venture capital providers and also find alternate sources of funding (such as bank lending) hard to come by. They often lack the required skills in marketing, in business management, in dealing with funding companies like VCs and in international business development necessary to grow a company to mid- or large scale. They often do not want to bring in external people if it substantially dilutes their equity or freedom to control their business.

6.2.4 15 different government delivery partners

Due to the complex nature of cyber space, improving the UK's cyber security involves a number of Government departments and agencies. This has led to many government agencies involved in promoting cyber security usage and development in the UK, leading to a proliferation of government initiatives. These initiatives are established for good reasons, and we accept that this situation is a common feature of governments, but it makes it difficult to drive joined-up thinking (albeit OCSIA is trying to tackle this). Firms in the sector find this is confusing.

6.2.5 GCHQ has poor understanding of the commercial aspects of the market

GCHQ is the recognised government technical authority for cyber security in the UK, with an international reputation. But its administration of the various certification schemes lacks commercial focus. Interestingly, both large defence primes and small SMEs made this observation.

Charging a flat rate fee per firm for CHECK scheme membership is one example. Such examples drive the view that CESG is disengaged with the business community. Its process to select suppliers to the pilot Cyber Incident Response scheme was criticised in our interviews as being at best opaque and at worst unfair. The lack of coherence with Common Criteria standards increases the compliance cost to small businesses. Several other examples were also given to us, which substantiate the sense that CESG is unaware of the impact its decisions have on small businesses.

"CESG has suffered historically from poor engagement with industry, which leads to uncertainty on how and where industry should invest."

Colin Robbins, Information Assurance Collaboration Group & Nexor

Another dimension of this is the relatively weak record in commercialising IP (particularly in comparison with the US's NSA). The US is generally more open about seeking to productise and/or develop its IP.

We accept that improving the situation for smaller suppliers may come at a cost. For example, introducing more complex charging arrangements for CHECK might result in higher cost of administration and increased fees. We suggest in this case that a revenue-based charging model might be workable, and more equitable.

6.2.6 SMEs feel excluded from the defence and general public sector

In the defence sector, SMEs find that they have a lack of direct routes to potential clients. Its procurement procedures are not easily understood and the prime contractors don't routinely pass on work unless they are missing a critical component for a bid. The accreditation processes from CESG are felt to be expensive, with uncertain returns.

"It's difficult to gain prime supplier status or even addition onto a framework agreement through government procurement when you are a specialist consultancy. It is clear that government procurement favours contracting work to the major SIs who in turn subcontract the specialist works to (smaller) organisations like us."

Charles White, IRM

There is also a widespread view amongst SME suppliers that the public sector in general is disinclined to work with SMEs. Small businesses dislike processes that increase their cost of sale as a proportion of contract value. Issues range from the small, such as Pre Qualification Questionnaires (PPQs) citing minimum annual revenues, to the structural, like the lack of a standard procurement approach across all government departments.

6.2.7 Many SMEs are services businesses

Growth potential for SME services businesses is limited by reliance on recruiting new talented &/or knowledgeable individuals, who are scarce. Services business are not, by their nature, easily scalable (in comparison to software, for example). It is difficult for SMEs to keep pace with market growth, as the availability of talent is constrained and the rate at which new staff can be on-boarded is similarly limited.

In order to achieve a size that provides the benefits of scale SME services firms consider acquisition much earlier in their life than products firms.

6.2.8 Lack of buyer knowledge (in non-defence markets)

Many buyers, from senior levels down, lack knowledge of all but the best-known, most established security technologies, and their understanding of cyber security threats and their consequences is similarly limited. They often do not understand why they should invest in, say, anything other than a rudimentary anti-virus product. This is particularly true of SME buyers, but it is by no means limited to them.

> "Not enough is being done for the UK SMB sector, in the way of educating them on the dangers of cyber crime and the ways to manage that danger."
>
> **Graeme Stewart, McAfee**

For example, the 2013 Information Security Breaches Survey reported that 42% of large organisations don't provide ongoing security awareness training. And 26% hadn't briefed their board on security risks in the last year. The rates are even lower for SMEs.

This poor market knowledge has an overall limiting effect on the market.

6.2.9 Lack of accreditation for suppliers to SME and consumer buyers

SME buyers and consumers generally use retail outlets and small resellers to purchase IT equipment. Security features, if they are deployed at all, are usually implemented by well-meaning but unqualified technicians. There is no widespread practitioner accreditation that would communicate at least a basic level of knowledge and expertise, which would give confidence to buyers.

6.3 OPPORTUNITIES

6.3.1 The UK is one of the largest and most sophisticated IT markets

The UK is the fifth largest IT market and is by a clear margin the biggest and most enthusiastic user of e-commerce, mobile computing, public cloud computing (software as a service) and social networking in Europe. As such, the UK presents a huge opportunity for anyone providing good or leading edge solutions in cyber security, and that is good for UK-based providers. That said, the UK is also one of the most fiercely fought over markets in the world, due in part to its size and in part to the UK's openness to solutions from overseas.

6.3.2 Government and commercial sector will increase investment during the next 5-10 years

Threats posed by cybercrime will increase – this will be an area in which government and commercial sector organisations will increase their investment during the next 5-10 years. A rising tide lifts all boats. PAC foresees however that the majority of the opportunity will be in selling to the commercial/private sector thanks in part to the Government ambition to limit its overall ICT spend.

UK government buys a considerable amount of cyber security solutions - not just defence/intelligence but for other central government, health services, and local government (e.g. education). Exploiting this (e.g. by joining the G-cloud programme) enables companies to open up a new area of opportunity.

6.3.3 Foreign direct investment could boost the UK sector

The UK's defence-related cooperation with its European partners, especially France, has never been so strong. The UK should attract French and other European companies, such as Thales and Cassidian, to invest further.

The UK also has strong ties with US defence suppliers – it is the only level 1 partner in the F-35 fighter programme. The UK could leverage its strong position to encourage cyber-related investment from Lockheed Martin and others.

Of course, this is a double-edged sword: attracting foreign direct investment is good for jobs creation, but it can also hamper growth of indigenous suppliers. The question is then whether FDI has an overall net positive impact on the market, which depends on the relative strength of FDI funds versus indigenous investment. Given that there are more large suppliers abroad it's more likely that FDI funding available will be higher.

6.3.4 SME sector potential

As we say in 6.2.8, there is a low level of knowledge of cyber security amongst buyers. This is particularly true of SMEs. However, the SME sector (as buyers) is one of the greatest areas of potential. If UK small and medium sized businesses increase awareness of the potential cyber threats facing their business, then this can drive levels of investment that we have not seen to date. The increasing dependence of small business on digital channels is the biggest driver behind this trend.

6.3.5 Services potential

Many indigenous UK suppliers are services-based. While there are barriers to growth for individual services companies, as we indicate in 6.2.7, growth may come from increasing the total number of services firms. The biggest opportunity for the UK cyber security sector may well lie in the provision of services rather than products – SME buyers tend not to care whether their anti-virus software is made in Russia or Rusholme, but when it comes to expertise, they want to work with someone local, should they have any urgent problems. They all need guidance in best practice, in what works and what doesn't, what is needed and what is not necessary.

6.3.6 Clusters drive SME engagement

There is still a lot of room to increase the awareness of the issue of cyber security among SMEs. BIS could drive the creation and/or sustenance of clusters, either directly or indirectly through organisations like the Chambers of Commerce and UKTI.

Regional cyber security supplier hubs can be an effective way to organise networking/education events, in conjunction with local government bodies or other interested parties (insurers, academia) to the benefit of both buy- and sell-side. The success of the Malvern cluster, for example, is driven by learning within the cluster firms, raising overall capability levels and benefiting both supply and buyer communities.

6.3.7 Potential to exploit UK security expertise in international markets, particularly US, Australia, Middle East.

UKTI is already pursuing an agenda to promote the UK cyber security sector to countries and organisations (government and private) who are purchasers of other security offerings from UK industry.

6.3.8 Potential to commercialise some of the intellectual property and expertise that sits within UK intelligence services such as GCHQ

GCHQ, MI5, CESG and others are commissioning and deploying technologies that can potentially be deployed in other environments (though note our caveats about the limited trickle down in section 7.3.1), which could lead to opportunities for the developer if suitably de-classified.

6.3.9 Potential opportunity to exploit cyber liability insurance

We consider that for businesses of all sizes, there is a trade-off between cost to deploy a cyber security solution and the cost of a security breach. As the UK is one of the major financial hubs in the world, then UK-based insurance companies could take a lead in offering insurance products to insure against cyber breaches. Furthermore, cyber security firms could reach out to insurance companies to craft partnership and deals whereby businesses deploying a particular product suite would benefit from reduced premiums on cyber breach insurance.

This is an idea that is in its infancy, and has limited traction to date. More research needs to be done to determine the likely purchase of policies, and whether compulsion (as in public liability insurance) would have an effect of increasing adoption of cyber security (in order to reduce premiums, for example).

6.4 THREATS

6.4.1 The biggest cyber security firms are from overseas

The biggest names in cyber security are almost all US-based: Generalists like IBM, HP, and specialists from Lockheed Martin and Raytheon to Symantec. The biggest tech firms bundling cyber security as part of their offerings are also US-based, including Amazon, Apple, Google and Microsoft.

This is the other side of the double-edged sword: FDI could threaten indigenous firms.

6.4.2 Overseas investors are better funded

There is a much bigger, better developed venture funding climate in the US. Israel is very focused on funding defence and leading edge high tech startups. It is also true that VCs in the US are very open to funding UK companies, but generally that means they end up in US hands. Furthermore, stock market valuations of tech companies tend to be higher in US and elsewhere, meaning that:

- overseas companies likely to acquire UK companies thus often diminishing the UK industry
- large overseas players can out-market UK companies through stronger marketing, better reach globally, more ‘feet on the street’ etc.

6.4.3 Brain drain

A dearth of skills could drive dependence on foreign capability.

Anecdotally we were told repeatedly that in some UK university courses (not just cyber security), half of PhD students are Chinese. This is perhaps a comment on the financial pressures that universities are under, as they seek out lucrative foreign students. But it also demonstrates the relative lack of UK STEM students generally, as well as increasing the likelihood of watching foreign talent leaving the UK having benefited from UK expertise.

6.4.4 Proliferation of overlapping accreditation/standards

The multiplicity of standards in cyber security is not UK-specific but it leads to increased costs for suppliers and confusion or reluctance for buyers – for small providers these costs can be prohibitive.

This is particularly an issue where international standards exist but are duplicated by or rejected in favour of local options. Suppliers are forced to choose between access to domestic customers or international markets, and SMEs in particular cannot afford to do both. It leads to cases where UK businesses can work with foreign governments and enterprises, but not those in their own country.

An oft-cited example is the convergence between CESG’s Commercial Product Assurance and the internationally recognised Common Criteria, seen by many suppliers as a major imperative, but moving slowly.

National, proprietary product assurance schemes, irrespective of how good they are, introduce additional costs, barriers to entry and challenges to business with no guaranteed return on investment if they are not also picked up by the buying community to built into the procurement frameworks. Governments should work to improve and support international standards that support the export ambitions of SMEs and maximise the return on investment while minimising the costs of accreditation

Piers Wilson, Tier-3

6.4.5 International competition

At present the UK is ranked highly as being a safe place to do e-business and as a centre of cyber security excellence. But as we saw in our international comparison, other countries are also keen to position themselves as leaders, and are promoting their own capabilities and secure business credentials. These promotional activities could lead them to overtake the UK, in fact or perception, damaging the UK's prospects. France, for example, takes an active role in promoting its domestic environment, and its indigenous suppliers, in international markets.

Investment in cyber security must be maintained, but this may be constrained by the UK economy growing more slowly than predicted, with a commensurate further tightening of budgets.

6.4.6 Enterprise opportunity driven led by overseas decision-makers

One of the challenges facing UK cyber security companies looking to sell into sectors such as manufacturing, utilities and professional services is that many of the companies in these sectors are under foreign ownership. Group decision-making is driven outside the UK and so contracts are likely to be signed with firms based elsewhere.

This may drive UK-based firms to export, in order to influence decision making abroad, but it does give an advantage to firms based in the parent country.

6.4.7 Cloud-delivered services are expected to be secure

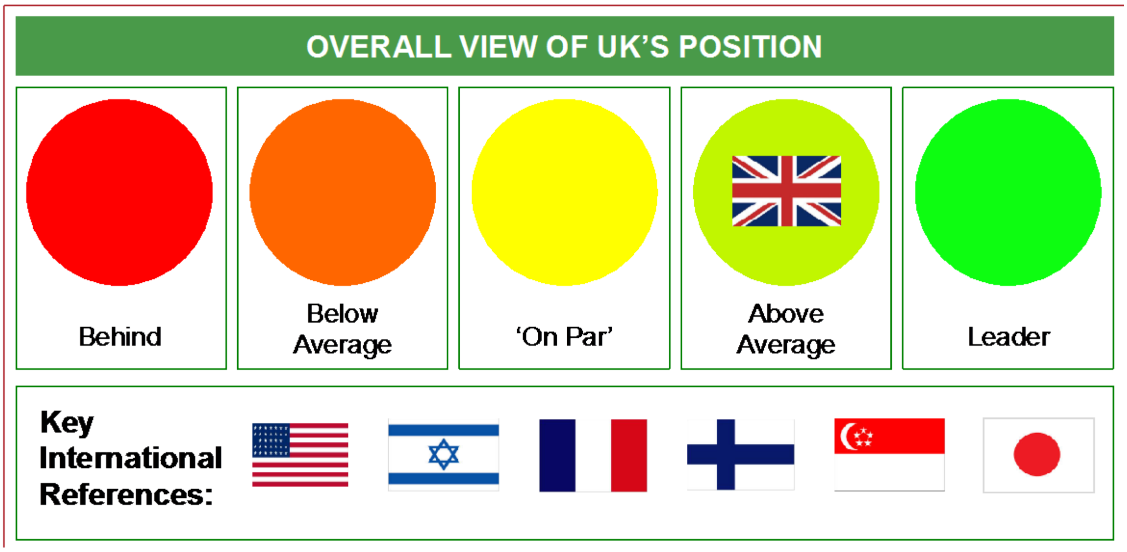
For many businesses, especially in the SME sector, there is an increasing expectation that services procured over the Internet (e.g. payments, email) are secured at source. Thus while those services provide a market opportunity, they may reduce the need for a separate and distinct security purchase by the services' recipient/buyers' organisation.

6.5 SWOT SUMMARY

STRENGTHS	WEAKNESSES
• The UK has world-class knowledge and companies	• Talent pool and supplier community is limited in size/number
• Large domestic market – with financial leverage	• Limited links between business and academia
•	
• GCHQ is an international star with a global brand and pedigree	• Many suppliers lack scale, know-how and funding
• UK university R&D is world class	• 15 different government delivery partners
• UK Aerospace & Defence industry is an asset	• GCHQ has poor understanding of the commercial aspects of the market
• Good public/private co-operation	• SMEs feel excluded from the defence and general public sector segments
	• Many SMEs are services businesses and find it hard to scale
OPPORTUNITIES	• Lack of buyer knowledge (in non-defence markets)
• The UK is one of the largest and most sophisticated IT markets	• Lack of accreditation for suppliers to SME and consumer buyers
• Government and commercial sector will increase investment	THREATS
• Foreign direct investment could boost the sector	• The biggest cyber security firms are from overseas
• SME sector potential	• Overseas investors are better funded
• Services potential	• Brain drain
• Clusters drive SME engagement	• Proliferation of overlapping accreditation/ standards
• Potential to exploit UK security expertise in international markets	• International competition
• Potential to commercialise IP and expertise within UK intelligence services	• Enterprise opportunity driven led by overseas decision-makers
• Potential opportunity to exploit cyber liability insurance	• Cloud-delivered services are expected to displace on-premise security solutions

7. Findings and recommendations

7.1 "ABOVE AVERAGE"



The analysis conducted for this report leads PAC to conclude that the UK's cyber security sector is above average strength on the world stage.. To use a cycling analogy, the UK is in the leading peloton, but there is no overall leader.

While there are certainly pockets of strength, such as managed security services and technical areas like cryptography, we find that:

- The US leads the way on cyber security spending with its enormous budgets, albeit its expenditure as a proportion of overall IT spending is similar to the UK or Germany

- The US also has the tech companies with the deepest pockets – Amazon, Apple, Google, Microsoft, Intel and others – who lead the way in R&D spend on security solutions linked to their general IT offerings, applicable in large degree to all markets: consumer & SMB, large enterprise, government and military. The US also leads the world in large generalist IT service and platform providers such as IBM, HP and Accenture, who have strong cyber security teams

- The US has a much better developed system of growing innovative tech startups (of all kinds) into medium and large companies through a much larger, more adventurous and more mature system of venture finance.

- France spends proportionately more on defence than the UK; it also has a cyber security sector of similar size and shape as the UK, and a strong programme of promoting home-grown solutions

- France also stands out for its strong generalist IT service providers – Capgemini, Atos, Steria – which have strength in this area sufficient for the needs of most mid-large sized enterprises which they can leverage with their clients in the UK and around Europe

- France is having success in getting its multinationals to pull in SMEs as partners in cyber security projects

- Israel stands out as a leader in small specialists; due to its political position and history, it has a very focused agenda to produce leading-edge solutions for the military/intelligence community (although like the UK, there is a long history of its best startups being acquired by larger overseas players mainly in the US).

- Singapore and Finland have particularly active national government programmes to publicise the importance of cyber security

- Japan is the second-largest spender on IT security solutions, both in absolute terms and as a proportion of overall IT spend.

In its favour, the UK has

- A number of global-scale, defence-oriented contractors, with world-class skills and recognized track records in general security and cyber security

- A few mid-sized specialists playing in the general commercial markets, who are holding their own but don't have particular USPs on the global stage

- A strong traditional defence industry whose business can be leveraged to sell cyber security to those countries and organisations where that traditional business is strong

- Several hundred small services and products providers with good and sometimes unique knowledge and IP in cyber security

- The fifth largest, and arguably the second most mature, market for IT products and services in the world, with particular pockets of need like financial services in the City of London; thus there is a proportionately high demand by organisations for cyber solutions to meet their particular needs

- A vibrant tech industry, particularly in certain specialist areas like mobile applications development centred in London, which will require local and often specialised support

- A considerable British cyber security skill-base within the UK operations of foreign-owned companies, such as IBM, HP, Capgemini, Lockheed Martin etc., and thus addressing many of the different market sub-segments
- Strong research, knowledge and track record in its universities, supported by government – but, very importantly, a poor track record in commercialising that research, and widespread indifference amongst SMEs toward using the results of academic research in their own businesses
- A growing awareness in the business and IT community at large about the importance of cyber security (albeit less knowledge on how best to respond).

The challenge for the UK cyber security sector, and for government, is to protect and nurture the industry, as there is considerable potential at home and overseas to be exploited – business that if the UK doesn't acquire it, overseas companies surely will.

Importantly, there has been an expectation in the past of a "trickle-down" effect in cyber security – that sophisticated solutions developed for defence and critical infrastructure providers will in due course be required by those further down the 'hierarchy of needs' and their developers will benefit from a wider market. However we find little evidence of that. It seems rather that large scale IT providers (mainly in the US) will incorporate the ideas and bundle them in their own products and services to service the less sophisticated needs of general enterprise, and then of consumers and SMEs.

In consequence we present the following recommendations.

7.2 RECOMMENDATIONS FOR GOVERNMENT

Base on our analysis of the market and feedback received from our extensive interview program we offer the following recommendations.

Our first two recommendations relate to expanding the demand side of cyber security through raising awareness. That said, we recognise that this will benefit all cyber security players. But a rising tide lifts all boats, and raised awareness contributes to government's other goal of making the UK a better place for e-business. The other recommendations are aimed at fostering a healthier indigenous UK cyber security supply side.

"The majority of SMEs have a view that (security breaches) will never happen to them. The problem is they are now the low hanging fruit for the hacker as the larger organisations are becoming more difficult to compromise. Most SMEs are also unaware of what defences they can use to make sure they are more secure"

Tony McDowell, Encription

7.2.1 BIS needs to be front and centre in raising awareness

BIS needs to further increase its visibility as HMG's lead department for cyber security awareness raising. It should continue to raise the issue with small to mid-size companies, who may be worried by media scare stories but don't know how to respond, or even don't really care. While we recognise that BIS has made some effort in this regard, for example through the '10 Steps' documents, a consistent and persistent programme is required. We think that this should be driven through SME ‘influencer’ bodies that have the reach and impact required.

Much of the work in raising awareness to date has been done directly by BIS, GCHQ and CPNI. This approach may be gaining traction with larger companies, but for SMEs the most effective channels of communication are likely to involve trusted third parties, such as ISPs, accountants, chambers of commerce and associations & forums.

BIS could also ensure that cyber security is a board level issue in larger organisations, where senior management may think it is fine to leave it to the CISO. BIS should work with the IoD and other board-level organisations to ensure board-level training courses are provided and widely sought-after. The cost of breaches is known to be high thanks to the BIS-sponsored “*Information security breaches survey*”.

“The security threat landscape has changed dramatically. The Government has taken positive steps in raising awareness, but many organisations still do not always understand in full what is valuable to their business, and how they should protect it .”

Dr. Bob Nowill, BT

Yet few companies put a value on a breach or loss of data – or even understand how to do this. BIS could disseminate more widely knowledge of the impact of breaches and popularise this amongst SMEs in particular. Ideally, an economic model of cyber risk that allowed finance directors to make appropriate provision would be valuable, and would gain board-level attention.

Insurance companies may have a role to play in valuations of cyber liability, although more research into this area is required.

7.2.2 BIS should help guide businesses to a list of approved suppliers for products and services

As well as pointing businesses towards GCHQ (CESG), BIS should promote approvals for suppliers and ‘kite-marking’ for e-commerce sites. BIS can justify such efforts on the basis of the potential cost to industry of data breaches (which is known, thanks to its *Information security breaches survey*) and the opportunity cost to the UK economy of business potentially being conducted elsewhere if local firms are not trusted to be secure.

Importantly, a basic level of accreditation, aimed at suppliers to SMEs and consumers, should be advanced. SMEs and consumers need to know that their suppliers are certified as knowledgeable and competent in cyber security. A scheme that is widely available and adopted is required, much in the same way as Checkatrade or GasSafe operate: CHECK and CREST have too few member companies[‡‡] to be scalable to the UK’s 4 million SMEs. Clearly such a scheme would offer far less rigour than existing schemes, but the requirements of SMEs and consumers are commensurately lower.

[‡‡] Both of these schemes have around 40 member firms.

7.2.3 Accelerate initiatives to ensure we do not have a talent shortage in the UK

As well as university courses, e-skills UK has launched apprenticeships in this area (with BT, Cassidian, IBM, QinetiQ and others). BIS should work with industry and other government departments to monitor success and encourage growth of this approach.

There needs to be an increased sense of urgency in this area. PhDs establish a core research capability, but they do not easily (or quickly) filter down into the workforce. MSc programmes are probably better suited to expanding the workforce rapidly.

In addition, more emphasis should be placed on practitioner certification at multiple levels. The top tier, in terms of capability, rigour and clearance, is well catered for, through the CESG Certified Professional (CCP) scheme. But certification for those professionals serving organisations with lower threat models are poorly served.

Post-graduate on-the-job training is not widely funded, though the TSB has provided funding for training, which is working well. One SME told us it costs £8,000 to train a new graduate in cyber security, on top of salary costs.

7.2.4 Recognise and capitalise on London as the main hub of cyber security suppliers

There is potential to develop ties between those vendors targeting businesses in key sectors such as financial services, utilities and manufacturing in terms of fostering joint marketing initiatives – particularly for the overseas market.

While there are other clusters of cyber security expertise, London is the largest and it is co-located with other complementary businesses and finance sources. More should be made of this situation.

7.2.5 Boost UK industry credentials by publicising the UK’s cyber security policies and agenda overseas

BIS shouldn't have to do this directly, but rather by encouraging ministers and other departments to build on the foundations we already have, such as the Foreign Secretary’s speech at the Budapest Conference.

Sustained effort is the key to publicising the UK’s credentials.

7.2.6 Support supply-side SMEs, which are vital for growth

The UK cyber security sector is primarily comprised of SME suppliers, and those SMEs require assistance that large organisations do not, both in terms of aiding the SME supplier community and in raising awareness across the potential SME buy-side. SME suppliers are most likely to benefit from an uplift in SME buyer cyber security adoption.

The large UK suppliers operating in this market are doing quite well on their own, and do not need much support with understanding markets and competition. Where the large contractors could always use more help is in (specific) opportunity identification and market intelligence about particular contracts, especially overseas.

Otherwise we think BIS should assist SMEs to grow, and the following recommendations are aimed at that goal.

7.2.7 BIS should expand its program to support SMEs' selling processes, e.g. through roadshow events

This is definitely something that should be escalated, and not just in terms of helping small cyber security companies engage with Government. The focus should be on how SME suppliers can engage with the larger technology suppliers that are typically the main route into enterprise accounts (large banks etc.). BIS should lean on big business and get them to do it on a pro-bono basis.

7.2.8 Support SMEs in understanding their market opportunities

Despite their success to date, most SMEs in the cyber security market do not have a clear picture of the shape of overseas markets, their potential prospects and their competition in adjacent markets. They are aware of this knowledge gap, but cannot individually afford to research this on limited budgets. BIS can help by sponsoring studies that can be provided to interested parties for an affordable sum or even free of charge.

7.2.9 Foster links between SME suppliers in the cyber security sector

BIS can help by facilitating SMEs talking to other SMEs about cyber security. Where this is happening already (e.g. Malvern) the SMEs find it valuable. Regional hubs would support better links.

"With (an increasing) emphasis now being placed on Cyber security, it would be advantageous for government procurement to more closely define the bidding lots and allow SME cyber security specialists to bid alongside the major SIs ""

Charles White, IRM

7.2.10 Expand initiatives to encourage more SME involvement in Government work

Government expenditure on IT (including security) is huge and it can influence through procurement. HMG is trying to get greater SME involvement in all aspects of IT supply; however there are still considerable barriers. BIS needs to explore how to ensure contracts with large players 'pull through' SME involvement, as expecting SMEs to become direct suppliers is often unrealistic, given the nature of Government procurement procedures. Ensuring large suppliers offer suitable commercial terms to SMEs should also sit within BIS's remit.

Certification is often cited by SMEs as a problematic, costly process. Look at new government processes and certifications that are more "SME-friendly." France is having success in getting its multinationals to pull in SMEs as partners in cyber security projects, and this example could be investigated further.

Part of the problem that SMEs face is simply gaining access to procurement information. Some tender documents are classified, requiring access to restricted (List X) facilities. Sponsorship by HMG is often required to attend briefings and networking events, and smaller firms find it hard to gain such backing. While much of this situation is inherent in the nature of HMG security policy, it remains a source of frustration for SMEs.

7.2.11 Improve SMEs' exploitation of university research knowledge, IP and skillsets

BIS should encourage initiatives that foster relationships between academia and industry, such as CSIT at Queen's University Belfast, and seek to develop more.

It should also further understand why industry is relatively dismissive of, or ignorant of, the benefits that using university resources could bring to their businesses and how to overcome barriers, and look into establishing new programmes to bring academia and business together in the cyber security space.

7.3 RECOMMENDATIONS FOR UK CYBER SECURITY PROVIDERS

7.3.1 Recognise that this isn't a single homogeneous market

As we have shown, there are different buyer submarkets, offering differing size and growth, and there are considerable issues involved in moving between them.

We have identified four distinct market types. The defence/intelligence sector is large but still a small part of the overall cyber security opportunity, both here and abroad. Moving into adjacent submarkets is not straightforward but can be worthwhile. The keys are to understand (a) what new skills you will require to operate in those markets and (b) what new competitors you will face.

7.3.2 Be aware of the impact of the Cloud on IT usage

As more IT is conducted using Cloud services companies, especially in the SME sector, will want fewer stand-alone security solutions, and will look for security-enabled cloud services. Your best opportunity may lie with bundling your capabilities with an e-commerce provider rather than selling directly to the user of that e-commerce solution.

7.3.3 Work with your peers to develop your reach and knowledge

The Malvern cyber partnership is a self-developed clustering mechanism that all participants agree has helped them in their business development. Explore – possibly together with agencies such as local Chambers of Commerce, BIS and UKTI – how to set up similar clusters in your own area. Even in the cyber age, geographic proximity can be an asset.

7.3.4 Look for the white space in the market

Look for white space, areas larger players haven't yet colonised. Don't try to create yet another malware / antivirus firewall solution when Microsoft (for one) gives such things away free.

The most promising areas to tackle are Managed Security Services and cloud-based solutions to exploit the general industry trends toward mobile, cloud-based, online and social network solutions in industries like retail, transport and hospitality, consumer and business services.

Another area to exploit is SCADA systems – post-Stuxnet it is recognised that these are vulnerable too, and there is a big gap in the market for solutions.

Look at providing 'solutions' rather than technology: SIEM, risk management, Unified Threat Management. Provide bundles of services and technology rather than one or the other.

7.3.5 Recognise that the defence/intelligence market is challenging

There's more money in the private sector, and routes to market in the defence sector are long, tortuous and difficult. If they seek you out, however, they will smooth the path for you.

7.3.6 Build alliances, partner or even merge

Midsize and large organisations have many advantages. These include economies of scale and (with the right partnerships) the ability to offer end-end solutions, from content to physical security. This is something many companies need but relatively few suppliers can provide.

Appendices

Appendix A – Research methodology

There were three primary input to our research process:

- Existing insight from PAC's SITSI Research program;
- Conducting primary research;
- Conducting secondary research.

A1. PAC'S SITSI RESEARCH PROGRAM

PAC has one of the world's most extensive data sets covering the software and IT services market globally. Our SITSI (Software and IT Services Industry) research program covers the full extent of software products and IT services, segmented into 15 discrete areas.

Within our SITSI research program we had in-house market figures for the UK, Western Europe and worldwide markets for the IT Security software and services segment. This data was a key input to sizing the cyber security market for the UK.

In addition, PAC tracks over 130 software and IT services firms worldwide, and a further 480 at country-level. We therefore have in-house one of the most extensive collections of market data on specific firms, many of which play in the cyber security market.

PAC has also conducted similar analyses of cyber security markets in France and Germany, and across the EU. Within the boundaries of clients' commercial confidence, we were able to apply our knowledge and understanding of the markets in these territories to this study.

A2. PRIMARY RESEARCH

PAC consultants conducted an extensive programme of face-to-face and telephone interviews. Interviewees were drawn from a broad range of industry suppliers and government stakeholders and we were facilitated in this process by industry bodies such as Intellect and ADS, as well as BIS.

We supplemented these interviews with a number of discussions with two key constituent groups identified by BIS: venture capitalists/investors and academics.

In all we conducted over 50 interviews typically lasting 1 hour (and often longer), making it a thorough investigation of the subject area. The interviewees and their organisations are listed in Appendix B.

In addition, we issued an online call for input. The purpose of the online call was not to conduct a statistically significant survey, but to offer as many firms as possible the opportunity to participate in our research.

This call was propagated via BIS, Intellect, ADS, the Malvern Cyber Security Group, Security Lancaster (at Lancaster University) and the Centre for Secure Information Technologies (CSIT) at Queen's University Belfast. Thirty-five firms completed our questionnaire.

A3. SECONDARY RESEARCH

We undertook a substantial statistical and literature review to identify studies previously conducted that examine local or regional trends in cyber security. This formed the basis for the International Comparative Analysis, as well as helping to inform our general view and recommendations in this report.

The sources we used are listed in Appendix C.

Appendix B – Market Sizing & Forecast Methodology

B1. MARKET SIZING

The sizing model for this report uses a combination of top down and bottom up measures. The top down model uses as its starting point our core SITS (Software & IT Services) framework[11], established over 20 years and proven to be reliable. Security-related SITS has been measured by PAC for the last 4 years, and again has proven to be reliable[12]. This provides an overall reference framework for the IT industry, and places certain constraints on any market sizing (such as the likely proportion of the IT market ascribed to cyber security).

To our SITS cyber security model we added in security-related hardware, network equipment and management consultancy fees to arrive at a first cut total market size for cyber security. Our numbers are calculated in euro: an exchange rate of 0.85902 was used to convert to GBP.

Our bottom up methodology required us to identify the total community of firms in the UK cyber security market. In all we identified 600 firms selling cyber security products and services in the UK, and determined or estimated their combined revenues in 2012. We use reliable (company published) data sources for our bottom up figures.

This exercise was more exhaustive than the majority of research exercises across the industry, and we are confident that these 600 firms form the vast bulk of the market. Almost half of these firms have revenues under £1 million, and so we can be confident that any firms outside the identified group will have revenues in this range (and thus would not affect our market sizing significantly).

We estimated that these 600 firms are responsible for around 90% of the cyber security market in the UK. The difference between our top down and bottom up market sizes is less than 1%.

B2. MARKET FORECAST

In order to predict growth rates for the various elements of the market we develop a scenario that encapsulates our assumptions of the key drivers and barriers to growth. Drivers have an overall positive impact on growth and barriers have a negative impact. Drivers and barriers may be internal to the market, such as shifts in security technology trends, or external, such as macro-economic influences. Clearly, drivers and barriers work in opposite directions, and so we determine the likely net effect on each of our segments. Our scenario is provided below.

Horizontal Domain	Short-Term Growth Outlook (2013)		Mid-Term Growth Outlook (2014-2015)		Long-Term Growth Outlook (2015-2017)	
	Drivers	Inhibitors	Drivers	Inhibitors	Drivers	Inhibitors
Project Services	Lack of skills drives need for external expertise Salaries commanded by CS experts is increasing in 2013 Demand driven by major banks, telcos, utilities and Defence/intelligence CS experts not attracted to in-house jobs in Government + Defence/intelligence so remain in external market Limited impact from offshore delivery models means rate pressure not as great as in wider application maintenance/dev services market Proliferation of cloud delivery models posing demand for advisory services on how to ensure data security/ownership issues and need to ensure that other departments understand new access/identity policies (HR)	Ongoing pressure on discretionary IT budgets Lack of awareness/ spending from SME companies	Ongoing lack of CS skills in-house drives services	Apprenticeship schemes begin to backfill skills shortages	Ongoing lack of CS skills in-house drives services	Pressure on skills may ease due to new CS graduate intake funded in 2013-2014

Horizontal Domain	Short-Term Growth Outlook (2013)		Mid-Term Growth Outlook (2014-2015)		Long-Term Growth Outlook (2015-2017)	
	Drivers	Inhibitors	Drivers	Inhibitors	Drivers	Inhibitors
Outsourcing	Managed firewall, monitoring and secure web access is externalized by many UK enterprises, with large telecoms providers and IT services generalists the chief beneficiaries	The number of large MSS opportunities coming out to tender remains relatively small compared to the wider IT outsourcing market (the large majority c80% of security-related outsourcing is "embedded" in a wider outsourcing deal) Concerns from some clients over loss of control over security processes Ongoing commoditization of network perimeter managed services (outsourced firewall management/IDS etc)	High cost and low efficiency of bodyshopping relationships encourages interest in more outcome-based, multi-year deals Increasing maturity of full-scope outsourcing propositions (covering threat identification, analysis, SIEM etc) makes external service providers more attractive, and deals get larger in size Mobile device security management an area clients increasingly looking to externalize	Concerns remain from some clients over loss of control over security processes	Increased appetite for standalone MSS engagements as clients look to work with best-of-breed supplier in multi-sourcing models Security-as-a-Service: some tools will be increasingly attractive as cloud-based services such as e-mail filtering	Concerns remain from some clients over loss of control over security processes
Software	Emerging softwre solutions consolidate point products	Commoditization of basic anti-virus software	Investment in threat analysis tools	Mature software products bundled free with hardware or services	Maturing solutions of pre-packaged software	Software increasingly delivered as a service
Hardware	Volume shipments increase as CS demand continues	Commoditization of hardware pricing - particularly in mature network perimeter device areas	Volume sustained due to replacement cycles	Commoditization of hardware pricing - particularly in mature network perimeter device areas, increase in services delivered via hosted platforms	Migration of on-premise kit into datacentres	Commoditization of hardware pricing - particularly in mature network perimeter device areas, increase in services delivered via hosted platforms

Vertical Domain	Short-Term Growth Outlook (2013)		Mid-Term Growth Outlook (2014-2015)		Long-Term Growth Outlook (2015-2017)	
	Drivers	Inhibitors	Drivers	Inhibitors	Drivers	Inhibitors
Defence/ intelligence	Positive impact of £650m Government National Cyber security Programme investment Increasing complexity of cyber-threats to national infrastructure	Defence and intelligence sectors struggle to retain best CS skills (from what is currently a limited talent pool) that are attracted by private sector remuneration	Positive impact of £650m Government National Cyber Security Programme investment (phased delivery) Increasing complexity of cyber-threats to national infrastructure requires more complex responses	Cessation of major infrastructure investment programmes in police national cybercrime centre etc Ongoing cuts to overall defence budgets	* Potential for the MoD budget to increase in the next parliament (if the 'budget black holes' unveiled in 2010 have been dealt with) due to implied requirement for the UK to resume its 'East of Suez' military role as the US gravitates more towards the pacific domain. * Several MoD outsourcing programmes are scheduled to coincide for renewal in order to allow a coherent forward approach. Security to be built in to a greater degree from hereon in?	Switch in focus away from cyber, or reappraisal of cyber as a a major threat
Rest of Government	* Government sector struggle to retain best CS skills that are attracted by private sector remuneration * G-Cloud initiative drives need to accredit smaller players to IL3 * Lessons learned from the London riots of 2011 leads public security agencies (incl. Police Forces, SOCA, MoD) to investigate social media security and analytics in order to enhance response times and identify threats	* Major budget cuts in local government (-20%), cost pressure faced within the healthcare segment * Fierce budgetary pressure is leading public sector organisations (especially in local government) to consider standardised and more flexible solution. Lack of budget to deal with existing challenges may prevent new investments in cyber security (at least on a significant scale). * Defeat of the 'Snoopers Charter' bill is likely to negatively impact the Government's planned activities in monitoring ISP traffic and social media networks.	* e-citizen agenda - in local & central goverment, education, health means many more systems are going online and thus need to be protected * I.e. expectation digital delivery of public services and growing use of public data to underpin public services (requiring security and citizen confidence) * Interest in outsourcing of security incident management (Government currently trialling on pilots with four providers)	* With the end of the parliament scheduled to fall in 2015, the Conservative Government may look to intensify its efficiency agenda for the remainder of the period in order to deliver on its budget deficit reduction targets. This may have a negative impact on expenditure, including cyber security.	* Cautious expectations of economic growth in the longer term may allow the government to reduce its austerity programme and increase expenditure in priority areas, of which cyber security is likely to be one.	* New government with new priorities * Faltering economy drives further budget constraints

Vertical Domain	Short-Term Growth Outlook (2013)		Mid-Term Growth Outlook (2014-2015)		Long-Term Growth Outlook (2015-2017)	
	Drivers	Inhibitors	Drivers	Inhibitors	Drivers	Inhibitors
Enterprise	Compliance requirements drive banks lead private sector in investing in encryption, SIEM technology In banking, vulnerability scanning & penetration testing, and threat management & monitoring services most commonly outsourced security processes.	Limited interest from retail sector - BRC 2012 report found that cost of customers put off by fraud prevention measures currently outweighs actual losses from fraud itself Lack of knowledge of impact/risk or solutions at Board level	Increased interest in security event monitoring as an outsourced service as clients understand the difficulty of doing this in-house Utility and manufacturing companies ramp up SCADA systems protection against cyber attacks Drive to move increasing number of IT workloads into the cloud increases the need for solutions and services to give adequate protection - and test for vulnerabilities etc Rising levels of e-commerce / online customer engagement and enterprise-supplier interaction solutions are altering the boundaries and making them necessarily porous to outsiders, making protection more difficult	Maturing adoption in key sectors such as finance	Increase in adoption by laggard sectors such as insurance & (business elements of) utilities	Maturing retail and manufacturing sectors

Vertical Domain	Short-Term Growth Outlook (2013)		Mid-Term Growth Outlook (2014-2015)		Long-Term Growth Outlook (2015-2017)	
	Drivers	Inhibitors	Drivers	Inhibitors	Drivers	Inhibitors
SME	Awareness of SME cyber threats increased by Information Security Breaches Survey £500k pot for CS technology for SMEs from Technology Strategy Board	Wider lack of awareness of cyber threats Lack of technical awareness of potential solutions, FUD about technology implementation Lack of access to SME-oriented services organizations with capability to implement solution	Awareness of threat increases driven by Government programmes such as GetSafeOnline SMEs' growing need and abilty to move their business online to communicate with customers and suppliers makes them increasingly vulnerable to cyber-attack	No imperative to implement security. Lack of measurable business risk inhibits adoption	Tools to size value at risk emerge. Insurance firms offer cyber clauses to liability insurance. Greater demand from consistent education and awareness programme. Several spectacular breaches and business failures drive adoption	Lack of standardised approaches to CS. No clear 'place to go' for CS advice. Conflicting, or ill-formed, standards. Shortage of SME-friendly (and affordable) advisers.
Consumer	Basic anti-virus packages often packaged with devices by retailers and manufacturers	Increasing commoditization and rising capablity of basic anti-virus tools and free solutions from Microsoft, Sophos etc	Bundled software on mobile and tablet devices	Diminishing propensity to pay for security features considered 'standard'	Education in CS factors increase awareness and demand	CS features embedded in cloud solutions as standard - no consumer demand for paid-for security

Appendix C – List of organisations interviewed for this study

We are grateful for the participation of the following organisations:

ADS
Amadeus Capital Partners
APM Group
Atos
BAE Systems Detica
BIS
BIS Local – South Central
Borwell
BT Cyber Assure
BT Defence & Security
Cabinet Office/OCSIA
CGI Group
Deep Secure
Digital Assurance
Digital Barriers
Encription Limited
EPSRC
Fidem
First Cyber Security
Get Safe Online
IBM
ICT KTN
Information Assurance Collaboration Group
Information Risk Management Plc
Intellect
Key-IQ
Kings College London
KPMG
Lancaster University
Malvern Cyber Security Group
McAfee
Microsoft
Nexor Limited
Notion Capital
nPulse Technologies
OBS
OSPL
Panmure Gordon
QinetiQ
Queen’s University Belfast
Quotium
Roke Manor Research
Royal Holloway College/University of London
Shadow National Cyber Crime Unit
Sophos
Sphericore
Symantec
Technology Strategy Board
Thales
Tier-3
Titania
UCL
UKTI
Verizon
Wipro
Zybert

Appendix D – Related documents

D1. REFERENCES

[1] Financial Times/ICSA Boardroom Bellwether survey July 2013. Only one in eight of the UK's largest 350 quoted companies claimed that they had seen and acted on the “10 steps to cyber security” guidance.

[2] ONS; Internet Access – Households and Individuals, 2012 statistical bulletin.

[3] Eric Luiijf et al, Nineteen National Cyber Security Strategies, International Journal of Critical Infrastructures, 2013

[4] Department for Business Innovation and Skills, 2013 Information Security Breaches Survey, 2013

[5] Bank of England Inflation Report May 2013

[6] UK Trade and Investment, Cyber Security: The UK's Approach to Exports, 2013

[7] EYGM Ltd, London–Globalizing venture capital: Global venture capital insights and trends report 2011

[8] KPMG, Data Loss Barometer: A Global Insight Into Lost and Stolen Informations, 2012

[9] IMF World Economic Outlook Database, 2013

[10] Boston Consulting Group, The $4.2 Trillion Opportunity: The Internet Economy in the G-20, 2012

[11] PAC, Software & IT Services by Vertical Sectors - Market Figures - Worldwide by Countries, 2013

[12] PAC, IT Security by Segments - Market Figures – UK, 2013

D2. BIBLIOGRAPHY

Aaron Kleiner et al, Linking Cybersecurity Policy and Performance', Microsoft Trustworthy Computing, 2013

Australian Government, Connecting With Confidence: Optimising Australia's Digital Future, 2011.

Australian Government, Critical Infrastructure Resilience Strategy', 2010.

Australian Government, Cyber Security Strategy, 2009

Booz Allen Hamilton and the Economist Intelligence Unit, Cyber Power Index', 2012, www.cyberhub.com

Cabinet Office, Progress Against the Objectives of the National Cyber Security Strategy – December 2012', 2012.

Cabinet Office, The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World', 2011.

CESG, '10 Steps to Cyber Security', 2012.

Dan Assaf, Models of Critical National Infrastructure Protection', International Journal of Critical Infrastructure Protection, 2008

Deloitte and the National Association of State Chief Information Officers, State Governments at Risk: a Call for Collaboration and Compliance', 2012.

Department of Defence (Australia), Defence White Paper 2013', 2013.

Dr Daniel Prince and Mr Nick King, Small Business Cyber Security Workshop 2013: Towards Digitally Secure Business Growth', 2013-06-10, funded by and produced in partnership with ICT KTN.

ENISA, National Cyber Security Strategies', 2012.

Executive Office of the President National Science and Technology Council, Trustworth Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program', 2011.

Executive Office of the President of the United States, The Comprehensive National Cybersecurity Initiative', 2010.

Federal Ministry of the Interior, Cyber Security Strategy for Germany', 2012.

Foreign & Commonwealth Office, Foreign Secretary Speech at the Budapest Conference on Cyberspace', https://www.gov.uk/ government/speeches/foreign-secretary-speech-at-the-budapest-conference-on-cyberspace

Geoff Dyer, Cyber Theft: A Hard Ware to Wage', Financial Times, 2013.

Government of Canada, Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada, 2010

Her Majesty's Government, Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review, 2010

IBM, IBM Internet Security Systems X-Force 2008 Trend & Risk Report', 2009.

IBM, IBM Security Solutions X-Force 2009 Trend and Risk Report', 2010.

IBM, IBM X-Force 2010 Trend and Risk Report', 2011.

IBM, IBM X-Force 2011 Trend and Risk Report', 2012.

IBM, IBM X-Force 2012 Trend and Risk Report', 2013.

Infocomm Development Authority of Singapore, Singapore's Strategy in Securing the Cyberspace, 2005

Information Security Policy Council (Japan), Information Security Strategy for Protecting the Nation', 2010.

Information Security Policy Council (Japan), Information Security 2012, 2012

Intelligence and Security Committee, Intelligence and Security Committee Annual Report 2011-12, 2012

Jeffrey Kuenzi, CRS Report for Congress: Science, Technology, Engineering and Mathematics (STEM) Education: Background, Federal Policy and Legislative Action, 2008

Kim-Kwang Raymond Choo, Cyber Security is a Team Sport', The Sydney Morning Herald, 2013.

Michel Rademaker, National Security Strategy of the Netherlands: An Innovative Approach, in Information & Security. An International Journal, 2009

Ministry of Security and Justice (Netherlands), The National Cyber Security Strategy (NCSS): Strength Through Cooperation, 2011

National Audit Office, The UK Cyber Security Strategy: Landscape Review, 2013

National Security Agency (US), NSA Technology Transfer Program', 2012.

Neil Robinson et al, Cyber-Security Threat Characterisation: A Rapid Comparative Analysis', Prepared for the Centre for Asymmetric Threat Studies (CATS), Swedish National Defence College.

OECD Digital Economy Papers, Cyber Security Policy Making at a Turning Point: Analysing a new Generation of National Cybersecurity Strategies for the Internet Economy, 2012

Office of the Secretary of Defence, Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013', 2013.

Parliament of Singapore, Computer Misuse (Amendment) Bill', 2012.

Pat Clawson, A Page From Singapore's Cybersecurity Playbook, 2009, http://blog.lumension.com/2249/a-page-from-singapores-cyber security-playbook/

Paul Cornish et al, Cyber Security and the UK's Critical National Infrastructure, Chatham House Report, 2011

Ponemon Institute (sponsored by Symantec), 2011 Cost of Data Breach Study: United Kingdom', 2012.

Post & Telestyrelsen, Strategy to Improve Internet Security in Sweden', 2006.

Prime Minister's Office (Israel), Cabinet Briefed on the Israel National Cyber Bureau', 2012, http://www.pmo.gov.il/English/MediaCenter/Spokesman/Pages/ spokecyber111112.aspx

Prime Minister's Office (Israel), Israel National Cyber Bureau and Ministry of Defense Directorate for Research & Development Announce Plan to Advance Dual Civilian-Defense R&D Projects', 2012, http://www.pmo.gov.il/English/MediaCenter/ Spokesman/Pages/spokemasad311012.aspx

Prime Minister's Office (Israel), Israel National Cyber Bureau Head Announces Launch of KIDMA', 2012, http://www.pmo.gov.il/English/MediaCenter/Spokesman/Pages/s pokekidma131112.aspx

Risk Based Security, Data Breach QuickView: An Executive's Guide to Data Breach Trends in 2012', 2013.

Secretariat General de la Defense Nationale (Office of the Prime Minister), From Crypto Control to Cyberdefense: An Overview of the French Defense and National Security Strategy in the Field of Cyberdefense', 2009.

Secretariat Generale de la Defence et de la Securite Nationale, Information Systems Defence and Security: France's Strategy', 2011.

Secretariat of the Security and Defence Committee', Finland's Cyber Security Strategy: Background Dossier', 2013.

Security & Defence Agenda, Cyber Security: The Vexed Question of Global Rules, 2012

Shmuel Even and David Siman-Tov, Cyber Warfare: Concepts and Strategic Trend', Institute for National Security Studies (Israel), 2012.

Stuart Sumner, Lack of Cohesion in UK Cyber Security Warns Former GCHQ/CESG Head, Computing Magazine, 2012

Symantec, Internet Security Threat Report', 2012.

Symantec, Internet Security Threat Report', 2013.

Technology Strategy Board, Ensuring Trust in Digital Services', 2011.

Technology, CRS Report for Congress: Science, Engineering and Mathematics (STEM) Education: Background, Federal Policy and Legislative Action'

Teodor Sommestad et al, SCADA System Cyber Security – A Comparison of Standards, 2010

Trustwave, 2013 Global Security Report', 2013.

Verizon, 2013 Data Breach Investigations Report', 2013.

White House, 'Strategic Plan for Federal Cybersecurity Research and Development Program'

Contributors

This report was written by:

Duncan Brown (Lead)
Philip Carnelley
Mathieu Poujol
Dominic Trott
Nick Mayes

Contact

Authored by:

Pierre Audoin Consultants (PAC) UK Ltd
15 Bowling Green Lane
London EC1R 0BD

T: +44 (0) 20 7251 2810
F: +44 (0) 20 7490 7335
E: info-uk@pac-online.com
www.pac-online.com

This publication is available from www.gov.uk/bis

Any enquiries regarding this publication should be sent to:

Department for Business, Innovation and Skills

1 Victoria Street

London SW1H 0ET

Tel: 020 7215 5000

If you require this publication in an alternative format, email enquiries@bis.gsi.gov.uk, or call 020 7215 5000.

BIS/13/1231