PROJECT ASPEN

A strategy for investment in global cyber security

EISVOGEL

Executive Summary

Global cyber security spending 2012: $60 billion

Forecast to reach $120 billion by 2017

Cyber crime costs the UK economy over £27 billion a year

Cyber criminals are now targeting the consumer…

Consumer cyber crime affects over 1.5 million victims daily

Cyber criminals have switched to targeting mobile platforms and social networks

Global mobile device security market estimated to be worth $14.4 billion by 2017

Secure mobile for consumers and business will become the new norm

There is currently no single commercial provider of effective integrated mobile security solutions in the UK or US market place

Project ASPEN is targeting small providers of niche security technologies to acquire an operating platform to consolidate further technologies, expertise and businesses in order to build a single integrated mobile security solutions capability provider

Introduction

In the last two decades, technology has dramatically changed the way the world communicates and does business. Traditional boundaries have shifted and we now operate in a dynamic environment that is increasingly interconnected, integrated and interdependent. The technological ecosystem is built around a model of open collaboration and trust – the very attributes now being exploited by an increasing number of criminals and, in extremis, global adversaries. Whilst the digital revolution has evolved the way we conduct our everyday activities it has also created a sophisticated and complex set of security issues.

Technology and the internet have become an integral part of everyday life and business. As key technologies become more pervasive government, business and individuals are becoming more dependent upon them for a variety of basic functions. Organisations and individuals now hold increasing amounts of sensitive information electronically and the ability to readily store and share this data across interconnected networks has created new efficiencies. It has also created critical exposure to new risks, which include computer-based fraud, the theft or manipulation of sensitive or private information and viruses that can destroy data, damage hardware and disrupt systems and operations.

The World Economic Forum describes this risk associated with these "cyber attacks" as one of the biggest risks that organsiations will face in the next decade. However, the potential impact of cyber attacks on individuals, businesses or organisations is often underestimated and not always fully understood. The proliferation of cyber attacks over the past decade has placed an increasing responsibility on companies and government organisations to become more aware and better prepared for the dangers exposed to them through under-protected networks or from individual negligence.

While cyber security risks have dramatically evolved, the approach individuals and businesses use to manage them has not kept pace. The traditional information security model does not address the realities of today. Effective and appropriate cyber security is critical if organisations and individuals are to operate effectively and prosper in our hyper-connected world.

The growing sophistication and range of cyber threats, and the increasing awareness of the risks and associated costs, is driving investment in the sector. There is already an active and growing volume of M&A activity. Traditional defence primes are seeking to expand their offerings to Governments, both to provide additional security services and to develop cyber tools that can be used both offensively and defensively against other technologies. Consumers and organsiations are demanding more from the companies that provide hardware and software; existing providers are looking for ways to gain more rapid access to emerging technologies that can differentiate their offerings with enhanced levels of security.

As the world becomes ever more connected and demanding of the benefits that unprecedented information sharing and communications creates, there is also a growing awareness of how vulnerable such extensive and complex networks can be. Vast amounts of data are available more readily to more people than ever before, but there is equal recognition that managing and securing the data explosion is increasingly difficult. The divide between work and home is blurring, with constantly connected mobile users now working in ways that create challenges for corporate IT departments in securing their systems without damaging productivity. Added to these trends are the specific impacts of e-finance, the emergence of tougher regulatory standards for data protection and privacy and the development of "new internets" of large private networks. Together these key trends are driving cyber security as a critical contemporary issue and reinforcing the sector as a major growth industry.

This short paper aims to provide an overview of the cyber security sector, defining what is encompassed by the term cyber and the nature of the threat that ultimately feeds it. It examines the key trends that are driving this rapidly evolving industry and, in conclusion, identifies specific sub-sectors and segments where we believe the most attractive opportunities for investors exist.

Defining "Cyber"

The broad term "cyber" encompasses more than just a technology and more than just the internet. It is a domain similar to that of land, air, sea, and space, but with its own distinct characteristics and challenges.

The cyber domain has national and international dimensions that include intellectual property, security, technology across industry, trade, culture, policy, and diplomacy. Operationally, it includes the creation, transmission, manipulation, and use of digital information. Technologically, it consists of all converged elements of electronic exchange, including voice, video, and data that involve the movement of electrons and photons across wired and wireless environments. The exchange takes place between devices of varying size and sophistication, such as desktops, laptops, smart phones, mainframes, televisions, radios, supervisory control and data acquisition (SCADA) systems and communications satellites. Convergence brings together digitised content (e.g., television programs, music, and books), digital devices, digital services, telecommunications, and cable into the increasingly interdependent and complex cyber domain, a domain that has little regard for traditional geographical or national boundaries.

The threat to this cyber domain is also global, pervasive, and growing exponentially. The threat, when realised, also bears a significant cost to the victim and one that extends far deeper than simply the direct financial cost of response and remedy. Victims of successful cyber attacks are likely to incur significant costs both in relation to remediation and repair, but also in reputational damage, litigation, loss of revenues and compensation. These costs may include notifying affected parties and/or regulators, hiring external advisers, paying fines imposed by regulators, defending or conducting litigation, restoring brand equity, and recreating lost, damaged or stolen data.

A cyber threat can be unintentional and intentional, targeted or no targeted, and can come from a variety of sources, including foreign sovereign nations engaged in espionage and information warfare, organised criminal groups, terrorist groups, hackers, virus writers, business competitors, and disgruntled employees and contractors working within an organization. Cyber threats by their very nature pervade national boundaries and legal systems. Cyber security encompasses all aspects of defending information and systems from risks such as cyber terrorism, cyber warfare, and cyber espionage. In their most disruptive form, cyber threats work to infiltrate and attack secret, political, military, or infrastructure assets of a nation and its people. Cyber security is consequently a critical part of any national security strategy. Most broadly cyber security is therefore the collection of tools, policies, security concepts, safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber domain and organisations and individuals data and hardware.

A recent report for the UK Government estimated that the cost to UK companies of cyber security breaches had tripled since 2012 and that attacks are costing the UK economy around £27 billion in losses annually. To give some context to the extent of the threat; around 90% of all British companies suffered some form of cyber attack in 2012. The US IT firm Symantec assesses the theft of intellectual property costs US companies in excess of $250 billion per year and estimates the total global cost of cybercrime at over $1 trillion. In response the UK, US, and other governments are investing heavily in raising cyber capability at national level and in critical supply chains and national infrastructure. The U.S. Federal Government has allotted over $13 billion annually to cyber security since late 2010 and the UK Government has now committed a further £210 million of investment in addition to the £650 million already allocated for its National Cyber Security Programme.

Recently there has been increasing global awareness, through well-publicised cases in the media, of the impact cyber attacks have had on both government and commercial organisations. Anti-virus vendors report increasing volumes of malware on the internet against which "patches" to software and applications have to be deployed (through regular software updates). Operating systems are a fruitful target, whether on mobile devices or computers.

The cyber security market broadly splits into two subsets. The first is the development of products and services for offensive applications. These are largely (if not exclusively) designed for government and

military use, and are often also referred to as cyber warfare or cyber attack and defence. The second encompasses the IT domain (primarily Internet Protocol or just 'Internet' connected devices), but also telecoms equipment and industrial equipment for both commercial and personal users.

The cyber security industry is comprised of companies that provide products and/or services for defensive and offensive applications across both the government and IT domains.

Market size and projected growth

Global cyber security spending was approximately $60 billion (£38.5 billion) in 2012 and is expected to grow at close to 10% annually over the next 3 to 5 years. Global Industry Analysts Inc put a headline figure on the sector of $80 billion (£51.3 billion) by 2017. Visiongain also estimates a global market size of around $60 billion (£38.5 billion) for the 2012 market but goes further to estimate that the market will reach $120 billion by 2017. The US accounts for over half of the total global revenues for cyber security. The next largest market is Japan, followed by the UK.

In most countries, the private corporate sector accounts for the majority of cyber security spending. The notable exception is the US where government spending is almost equal to that of the private sector. US Federal Government spending is around $13 billion per annum, with a CAGR of 6.2% over the period 2013-2018.

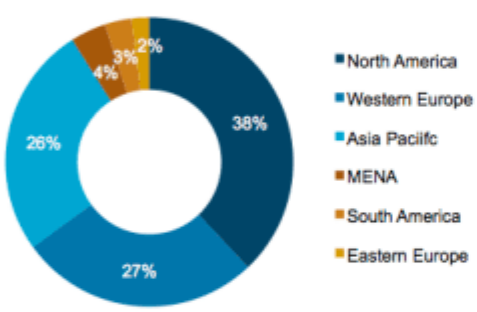


Fig 1: Cyber Security Market: Global Spending by Region 2011.

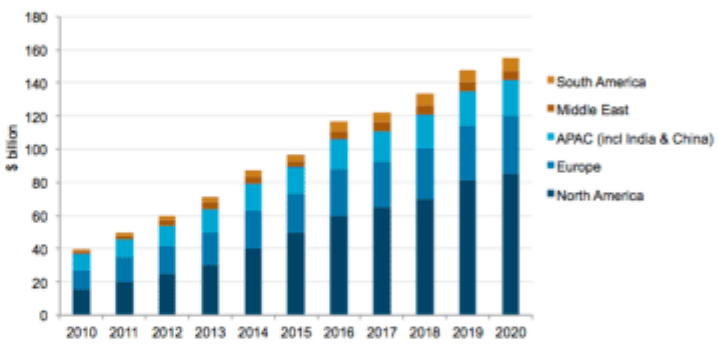


Fig 2: Global Cyber Security Market Revenues 2010-2020.

Governments typically spend a higher than average percentage of their overall IT budget on security and cyber than the private sector because of their enhanced need to protect their information. Moreover, because of their more demanding architectural needs their IT systems typically cost more than those in the private sector. Our estimate is that the UK government spends around £12 billion per annum on IT and around £1bn per annum on IT security, including cyber security measures. Furthermore the UK government is making increased spending commitments to its National Cyber Security Programme, which is intended to improve capacity and capability in government, supply chain and society on both defensive and offensive capability. In addition, certain government agencies in both the UK and US are devoting more of their internal resources to this growing problem – achieving this capability will require technology solutions and support.

The private sector generally is a far larger market. Spending in the UK is currently around £60 billion per annum on IT but less as a proportion on cyber and system security. Our estimate is that the private sector typically spend around 5% to 7% of their IT budgets on security, suggesting an annual spend of around £3 to £5 billion. The private sector's cyber security needs are different to government, focusing more on the protection of assets, whether customer data or IP, and having a resilient infrastructure that ensures robust productivity and commercial resilience.

Recent high profile security breaches and subtle yet aggressive corporate espionage cases have highlighted the scale of the threat faced by business from cyber security attacks. Commercial organisations must now accept that this issue is no longer the preserve of IT departments and the CIO. The simultaneous benefits and vulnerabilities inherent in digital networks are board level issues. One of the key problems is the fact that organsisations may not be immediately aware that they have been the target or the victim of an attack. Direct targeting of intellectual property, theft of customer and client information, vulnerability of supply chains, and reputational protection for both customers and shareholders are among the critical risks faced by organsiations on a daily basis. In the UK alone an average of 33,000 malicious emails a month, containing sophisticated malware, are blocked at the gateway to the Government Secure Intranet. In addition, a far greater number of less malicious threats, comprising less sophisticated malware and spam, are blocked by the UK Government on a monthly basis.

There have been a number of high profile cyber security incidents this year alone, from computer hacking groups, such as LulzSec's attack on the Sony Playstation network to foreign intelligence services, including an attack in March where 24,000 confidential files were stolen from a Pentagon defence contractor. More recently, quasi-political activist groups such as Anonymous have targeted a range of high-profile businesses and organisations. The apparent ease with which some of these activities have taken place has very publicly highlighted the importance of effective cyber security. The costs arising from such breaches have also focused corporate attention on security. Sony reported that the hack of its PlayStation network and the consequent loss of its network availability will cost its business over $170 million.

Viruses have also been developed to attack specific types of equipment. The Stuxnet virus, for example, aimed at industrial control systems, was largely attributed with the problems that hit key Iranian nuclear facilities, impacting its uranium enrichment programme. On a more personal, but no less sensational, level, the breach of individuals' mobile phone voicemail accounts by reporters from a News Corporation publication, The News of the World, has also highlighted the vulnerability of telecoms and other personal mobile equipment to unauthorised access.

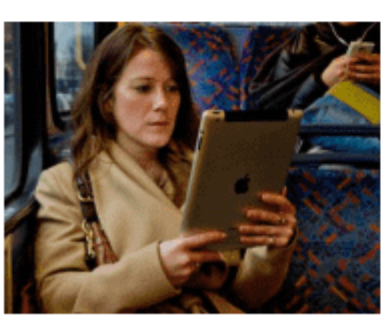
Against this backdrop of growing threats deal activity continues to increase. Cumulative global corporate spending on cyber security deals since 2008 totals nearly $22 billion, an average of over $6 billion in each year. Acquirers have been from a range of sectors including technology, IT services, aerospace & defence as well as financial investors. Much of this activity is being driven by the large global defence primes who's traditional global aerospace and defence markets are worth around $450 billion. However, revenues in the traditional defence sector are not expected to show much growth over the next decade at least, so the cyber security represents a significant opportunity for the defence majors. Many have already grasped this opportunity through acquisition as well as building on, and organically growing, their own in-house cyber security solutions. BAE Systems purchased Detica for £531 million and Boeing has acquired up a range of specialist providers, such as Narus Inc and SMSi. BAE and Safran shared a purchase of L-1 Identity Solutions, and Raytheon has spent over $1 billion on a range of smaller cyber companies over the past four years. QinetiQ, an important player in Europe, has also made several acquisitions.

1	***IT Infrastructure revolution***	▪ Increase in penetration if high speed and wireless networks. ▪ Centralisation of IT resources and adoption of cloud computing. ▪ Proliferation of IP connected devices and growth in functionality. ▪ Improved global ICT infrastructure. ▪ Device convergence. ▪ Erosion of work/social division in personal IT – "Bring Your Own" approach to enterprise IT. ▪ Evolution in user interfaces and emergence of disruptive technologies.
2	***Explosion of "Big Data"***	▪ Greater sharing of sensitive data between organisations and individuals. ▪ Significant increase in visual data. ▪ Greater number of the worlds population connected. ▪ Greater volume of automated traffic from devices. ▪ Multiplication of devices and applications generating traffic. ▪ Greater need for the classification of data. ▪ More data being stored "at rest" on ever higher capacity devices.
3	***Always-on and always-connected world***	▪ Greater connectivity between people driven by social networking devices. ▪ Increasing connectivity between devices. ▪ Increasing information connectivity and data mining. ▪ Increased Critical National Infrastructure and public services connectivity.
4	***Future finance***	▪ Rising levels of electronic and mobile commerce and banking. ▪ Development of new banking models. ▪ Growth in new payment models. ▪ Emergence of digital cash.
5	***Law, regulations and standards***	▪ Increasing legal protection and regulation relating to privacy. ▪ Increasing standards on information security. ▪ Nationally imposed standards for industry. ▪ Globalisation as an opposing force to increased national regulation.
6	***More than one internet***	▪ Greater censorship. ▪ Political motivations driving new state/regional internets. ▪ New and more secure intranets. ▪ Closed social networks. ▪ Growth in paid content.
7	***New identity and trust models***	▪ The effectiveness of current identity concepts continues to decline. ▪ Identity becomes increasingly important in the move from perimeter to information based security. ▪ New models of trust develop for people, infrastructure, including devices and data.

Fig 3: Key trends and drivers in the cyber security sector.

The cyber market has, to date, been mainly dominated by large-scale corporations responding to the increasing demand from the Government sector. This capability requirement has traditionally been met by the large US and UK defence primes, including companies such as Lockheed Martin, General Dynamics, Northrop Grumman and BAE. Some of the most prominent traditional information technology sector players have also been engaged in the cyber domain as well as the traditional security software product providers such as MacAfee and Symantec. Hewlett Packard, IBM, CSC, CGI, Unisys, Cap Gemini and the large telecoms integrators such as Siemens and BT have increasingly large cyber capabilities. Together these major companies dominate the government and larger scale corporate sector. They are primarily focused on delivering cyber as a managed service including the network and security operating centers that actively manage the infrastructures that they are contracted to deliver.

Going mobile – the exploding trend



We live in an increasingly connected and mobile world. In recent years, there has been a fundamental transformation of the mobile ecosystem. Evolving technologies are presenting new opportunities for applications. Smartphones, tablets, portable gaming consoles, digital media players and cameras can deliver powerful integrated computing functionality which only desktop computers were capable of less than a decade ago. Mobile devices have been transformed into a multi-purpose utility with multimedia capability, delivering critical tools for personal expression, enterprise and entertainment. Mobile devices are now used for video

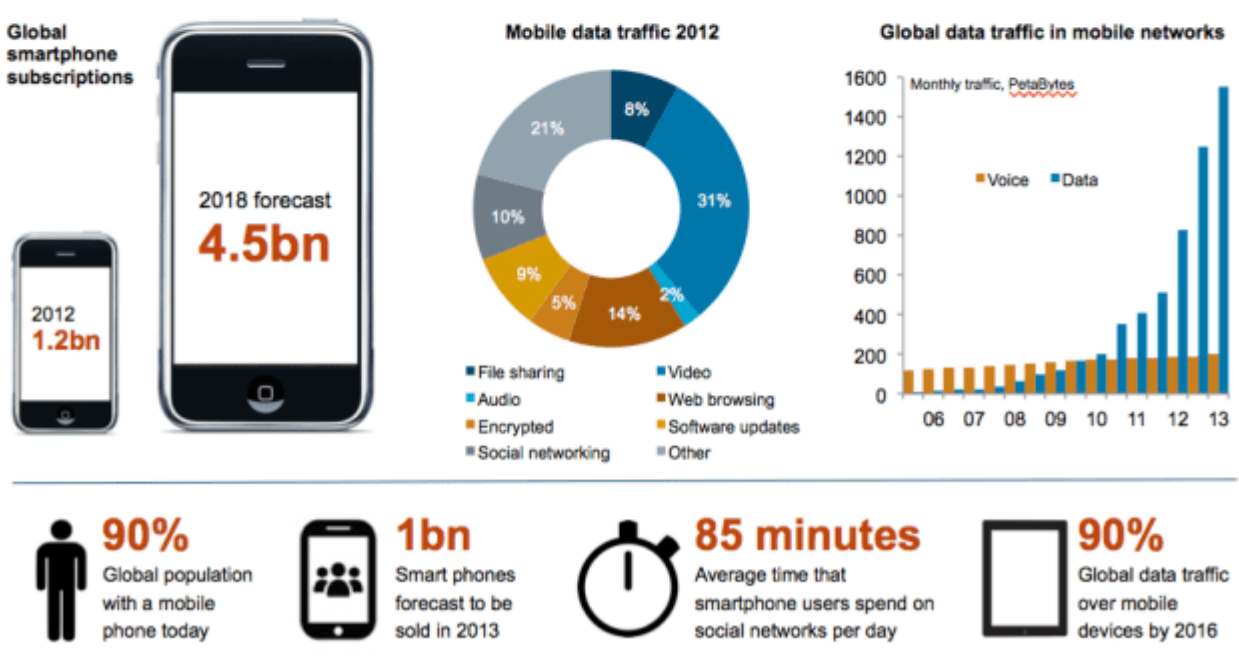
conferencing, storing documents and media, sending and receiving messages, online banking, gaming, navigation, shopping and other entertainment purposes. Many individuals, and in particular the younger generation, now rely on their mobile device to act as their digital identity for a carrying out a number of critical daily operations, such as completing financial transactions, and as a way of communicating within their social network.

Since the launch of devices like BlackBerry and iPhone, the smartphone and tablet market has rapidly evolved in three key areas: technology (better hardware and more optimized software), market (sales, number of users, number of applications), and connectivity and infrastructure (3G and 4G LTE). This sector has experienced considerable growth as opposed to "traditional" computer markets, whose sales have seen significant reductions as a result of the growth of mobile devices. While the traditional PC market has experienced a year-on-year decline of 11.2% (as of the first quarter of 2013), mobile device (netbook, smartphone and tablet) shipments exceeded 300 million devices in the first quarter alone, a year-on-year growth rate of 37.4% during the same period. A total of over 1 billion smartphones are expected to be sold in 2013, compared to the 700 million smartphones that were shipped in total in 2012, in itself a 43% increase over 2011's numbers.

The increasing adoption and the roll-out of more powerful mobile data networks (for example 4G LTE) in many regions will increase the availability of broadband and parallel services such as e-commerce, mobile payments, mobile banking, access to cloud services, video streaming and content download. Availability of such services further reinforce the critical role of mobile devices as well as increase the "attack surface" – the vulnerability and exposure to attack.

In 2013, for the first time, the number of people accessing the internet via a mobile device will be greater than those who use a PC. This distinct and measurable shift towards the use of mobile devices, such as phones and tablets, replacing PCs as the primary method of accessing the internet presents clear opportunities for individuals and organisations to exploit the benefits of mobile and cloud technologies.

Worldwide smartphone sales are forecast to hit one billion units in 2013 while connection speeds are forecast to rise sevenfold by 2017. Despite the scale of adoption of mobile devices there are still 5 billion global mobile phone users, which suggests that the growth in the total number of smart phone users still has some way to go. Networks are becoming more robust and able to handle larger and larger volumes of data. The number of networked devices is estimated to outnumber people by six to one, transforming our current conceptions of the internet.



Together with the rise in smartphones sales, the number of mobile applications downloaded from Google Play and Apple Store have also increased over the same period of time. In July 2011, 15 billion downloads from Apple Store were registered globally, while in March 2012, this number had almost doubled to 25 billion with a total of 550,000 available applications for iPhone, iPod and iPad. In the case of Google Play, the figures indicate a similar growth rate: in September 2012, the service reached 25 billion downloads around the world and a total of 675,000 applications and games. At the same time, 1.3 million Android devices are activated every day. Mobile devices (tablets and smartphones) have rapidly evolved in terms of both hardware and software. The market now offers smartphones with quad-core processors, increased RAM, more advanced graphic processors and other features that allow more complex tasks than was ever possible before. At the same time, new versions of operating systems like iOS, Android and Windows Phone have improved in areas like usability, functionality and performance. Society has increasingly adopted this mobile equipment with the intention of staying connected to family, friends, and work; consuming gaming or informative content; streamlining banking operations; and so on. The volume of malware designed for mobile devices is a direct response to the speed at which technology is being adopted. As this market grows and technology is enhanced, and as users store increasing amounts of sensitive information and use their devices to complete critical tasks, while not adopting the necessary security measures, the threats designed to exploit them will continue to grow in parallel.

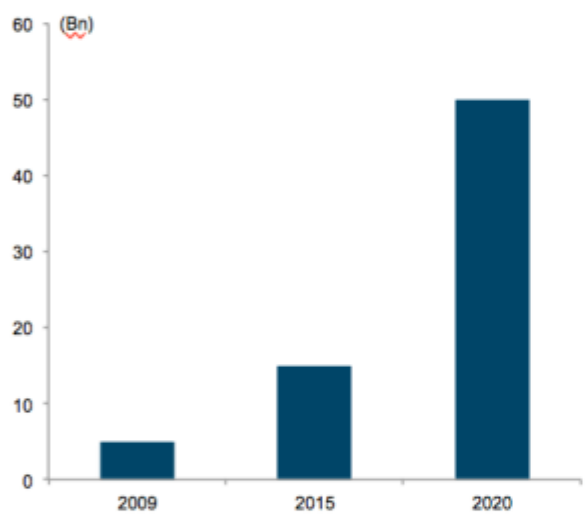


Fig 4: Global total number of devices connected to the internet.

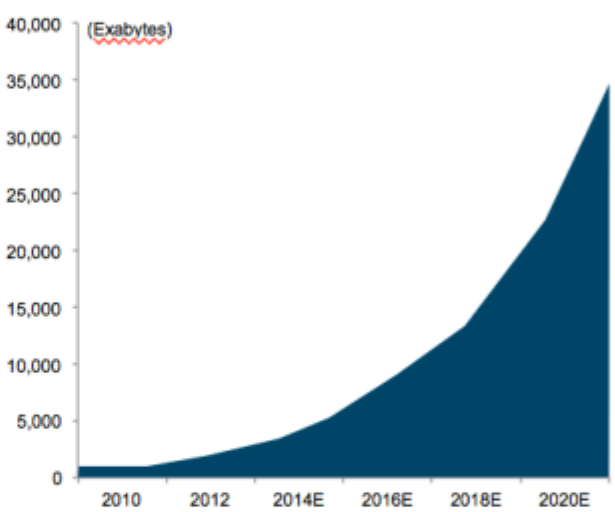


Fig 5: Total global digital data (exabytes).

In the workplace the lines between personal and professional technology, home and office are blurring. Increasing numbers of organisations are allowing employees to bring or choose their own devices (BYOD) or are providing them with smart phones, laptops and tablets to work and to access sensitive information on the move. The BYOD phenomenon is directly related to the development of increasingly advanced mobile devices and applications. BYOD implies that a company's employees can carry and use personal devices such as laptops, smartphones and tablets within the corporate environment (including access to Wi-Fi wireless networks, VPNs, shared files and printers, among others). In the UK 87% of large organisations and 65% of small businesses now allow mobile devices to connect to their systems remotely. It saves money, increases efficiency and attracts and retains staff. Intel, for example, calculates that employees using their own devices save up to 50 minutes a day and that productivity gains will be worth $177 million this year. Consequently, unless the necessary security measures are taken, BYOD can introduce significant security threats. For example, an employee could have access to all his employer's corporate resources through a smartphone that is infected with a malicious program, and that program could steal the organisation's confidential information. Another problem that may arise as a result of this trend is the theft or loss of a mobile device; therefore, if it is not properly protected, a third party could access the sensitive data stored on or accessible via the device. The consumerisation of IT is one of the biggest challenges facing businesses and government departments worldwide and whilst there are clear business benefits from the use of mobile devices, companies also need to be aware of the critical data loss and security risks

associated with them. As mobile devices become even more pervasive and store more personal and corporate data, new tools to secure that information will drive the mobile-security market.

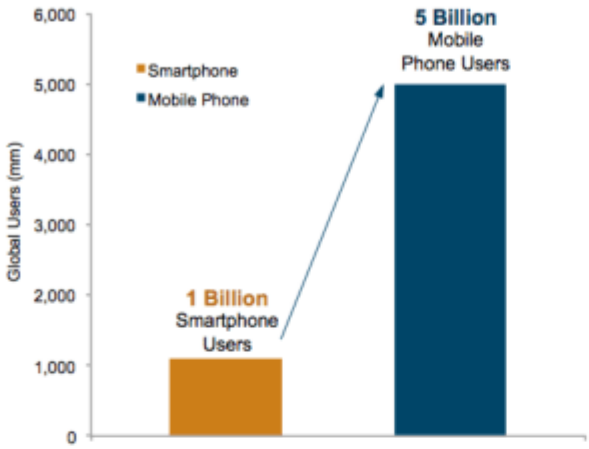


Fig 6: Global Smartphone and Mobile Phone Users 2012.

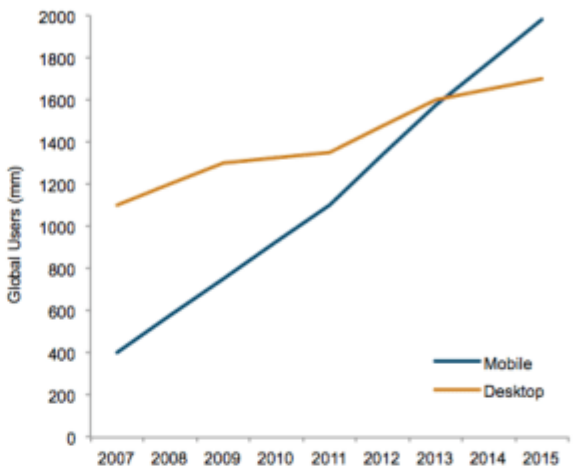


Fig 7: Global mobile vs. desktop internet users 2007-2015.

Companies are also increasingly adopting remotely hosted services in the cloud as an affordable and easily accessible alternative to internal IT systems. Over 80% of UK companies are now using at least one cloud computing service. Website and email remain the most commonly used services, particularly for small businesses, where the majority of websites are external and many use an externally hosted email solution. The biggest rise in cloud computing usage has been data storage on the cloud and increasing numbers of companies are storing confidential data on the Internet. Both large and small organisations have confidential or highly confidential data on the cloud. Though cloud computing remains in its infancy, security and privacy issues have been magnified by the velocity, volume and variety that it presents. The use of large scale cloud infrastructures, with a diversity of software platforms, spread across large networks, also increase the attack surface of the entire system.

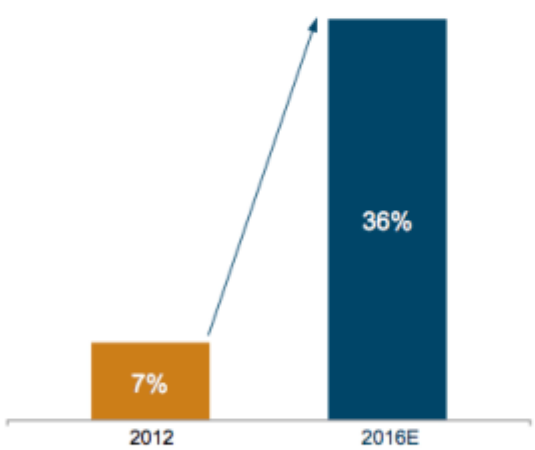
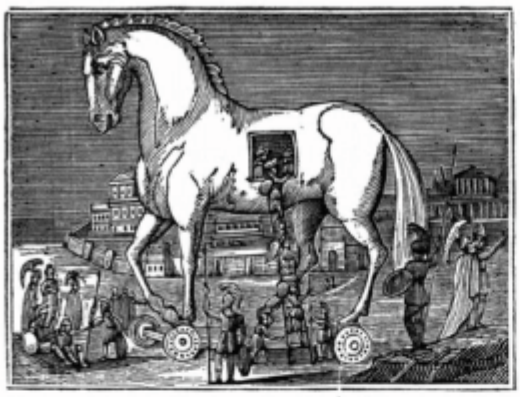


Fig 8: Growth in total number of files belonging to end-users stored in the cloud.

The increased risk to personal and corporate data is the key opportunity for the mobile-security industry. The global market for mobile security is expected to reach $14.4 billion by 2017. Issues such as data breaches, unauthorised access to and loss of personal information stored within the mobile phone, malware and malicious applications all highlight the need for more comprehensive and effective mobile security.

When it comes to protecting the enterprise, IT departments are also increasingly looking beyond basic, simple security applications; demand for specialized services is beginning to drive the market. Network security, managed security and professional services are set to become the biggest categories for business-to-business mobile security. Bundled network security, which includes unified threat management, deep packet inspection, virtual private networks and remote device management, will become ever more important. Increasingly, mobile security is concentrating on services for mobile devices, identity and authentication management, as well as for audits, certification and consulting.

Growing threats and increasing awareness



Trojans Deceived.

As mobile devices proliferate so do the number of threats designed specifically to exploit them. In the first six months of 2013 the number of unique mobile threats has grown by 261%. Increasingly complex malware is taking advantage of the wider range of mobile functionalities and are specifically deployed to exploit vulnerabilities on the device and in the network.

At the start of 2013, researchers at the anti virus software company McAfee Labs identified 36,699 mobile malware samples. 95% of those samples only appeared over the course of the previous 12 months. In comparison, McAfee threat researchers gathered just 792 samples of mobile malware in total during 2011. Kaspersky Lab, a competitor to McAfee, identified a total of 22,750 new modifications of malicious programs targeting mobile devices during Q1 2013. This is in comparison to a total of 40,059 modifications of malicious programs targeting mobile devices detected over the whole of 2012. 99.9% of the threats identified targeted the Android platform (Android remains the preferred operating system in more price-sensitive markets such as Asia and Latin America).

The most prevalent category of mobile threats is that of SMS trojans, which send unauthorized text messages to short, premium-rate numbers. Other threats include information theft (spyware), and the transformation of machines into zombies (botnet recruitment). Many trojans target internet users attempting to download software for their mobile devices from dubious sites. Often, cybercriminals use these websites to spread malware under the guise of useful software. "Adware" trojans are used by the developers of free software to monetize products by displaying ads. Cyber criminals are able to disguise malicious programs as new versions of other popular apps (e.g. Skype, Angry Birds).

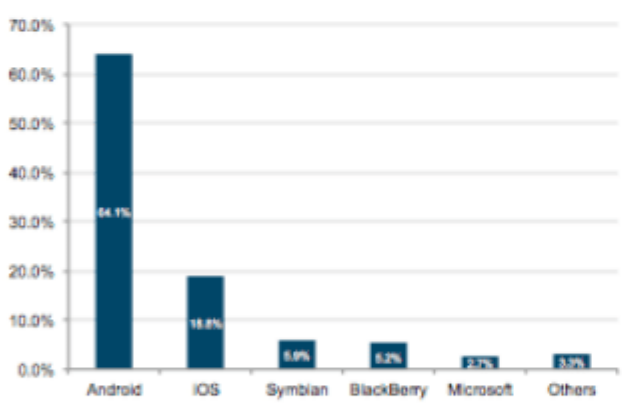


Fig 9: Smartphone sales to end users by operating system in the Second Quarter of 2012

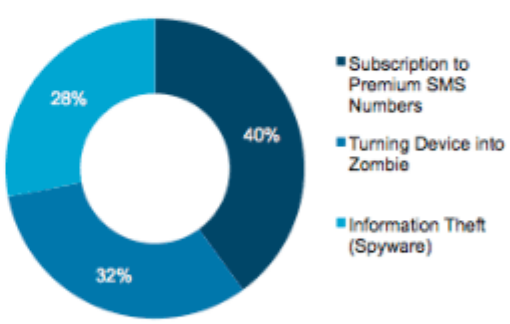


Fig 10: 2012 Threat Families and Malicious Actions (Payloads).

There have been two notable incidents in Q1 2013 involving mobile malware: In the first two weeks of March a new banking trojan targeting mobile devices, and allegedly affecting users in 69 countries, was identified. Dubbed Perkel it was designed to steal text messages containing mTANs (online banking transaction references). The second is the MTK Botnet, which by mid-January had infected up to one million Android devices owned primarily by Chinese users. The trojan spread via unofficial Chinese app stores with popular, cracked games. In addition to stealing information about the infected smartphone, user contact data and messages, threats in this family also send out false ratings on a variety of applications. To do so, the trojans stealthily download and install apps on the victim's mobile device, and then give that app the highest possible rating in the app store. Then, they report their actions to a remote server.

Incredibly only 4% of smartphones shipped in 2010 were sold with any form of pre-installed security

software. A similar study in the UK in 2011 identified that only 5% of smartphones and tablets had third-party security software installed on them. It is estimated that given the nature of the extant vulnerabilities and emerging threats that this number will grow rapidly, with some within the industry estimating that this will grow to as much as 20% of all mobile users installing some form of third party security software in the next 24 months.

Market opportunity

The growing number of threats targeting mobile devices and the exponential growth that both the devices and accompanying malware are experiencing present a clear opportunity in the confluence of cyber and mobile trends. Recent global media coverage of widespread interception by Governments of voice and data traffic suggests that the market for stronger encryption of private and corporate communications will strengthen as consumers seek to protect their privacy from both Government and non-state criminal activity.

The established and dominant market players within the broad cyber security market are currently characterised by those traditional defence primes and larger technology companies that are predominately focused on serving government and large-scale corporate customers and securing large enterprise networks. This level of the market is relatively mature and saturated. These larger players compete for share within a large and relatively well-defined government and corporate market. They are able to respond to the bespoke requirements of their key customers and will generally offer a tailored range of high value products and services. The market here is large and growing. Consequently it is highly competitive, with critical requirement placed on scale and experience to be able to deliver to government and large corporate customers. Despite the growth in the overall size of the market we judge that the field of defence contractors selling data-protection contracts to government and large corporate customers will actually shrink as increasingly sophisticated demands from clients push out some competitors.

Conversely the consumer and smaller business customer remains relatively under-served, with a number of smaller product offerings, predominately limited to anti-virus and anti-malware software. This, in our analysis, is the most attractive segment of the market, given the sheer scale of potential end-users directly correlated with the estimated number of smart phone and tablet users and growing vulnerability of the consumer to the widening range of threats.

The increasing proliferation of mobile internet devices and associated vulnerabilities creates a market for complementary mobile services in management and security in six mobile security sub-sectors:

- Mobile Data Security.
- Mobile Device Security.
- Mobile Virtual Private Network (mVPN).
- Mobile Identity Management (MIM).
- Mobile Device Management (MDM).
- Mobile Security as a Service (mSaaS).

There is currently no single commercial provider of effective integrated mobile security solutions in the market. Consumer understanding of the threats is growing yet there remains a critical gap in the market for an accessible, easy-to-use and affordable solutions product specifically targeted at the consumer mobile device user. We therefore believe that there is presently a clear opportunity to leverage the expertise developed in the high-end offensive and defensive applications of the US/UK military and government agencies and large defence primes and apply in a consumer focused solutions business, to provide a mobile device security capability that goes much further than the simple anti-virus apps currently available in the market. We believe that in the future secure mobile communications will be the norm and that all data across devices will be secured in some way. Device users will look back to this period of widespread insecure data communications as exceptional.

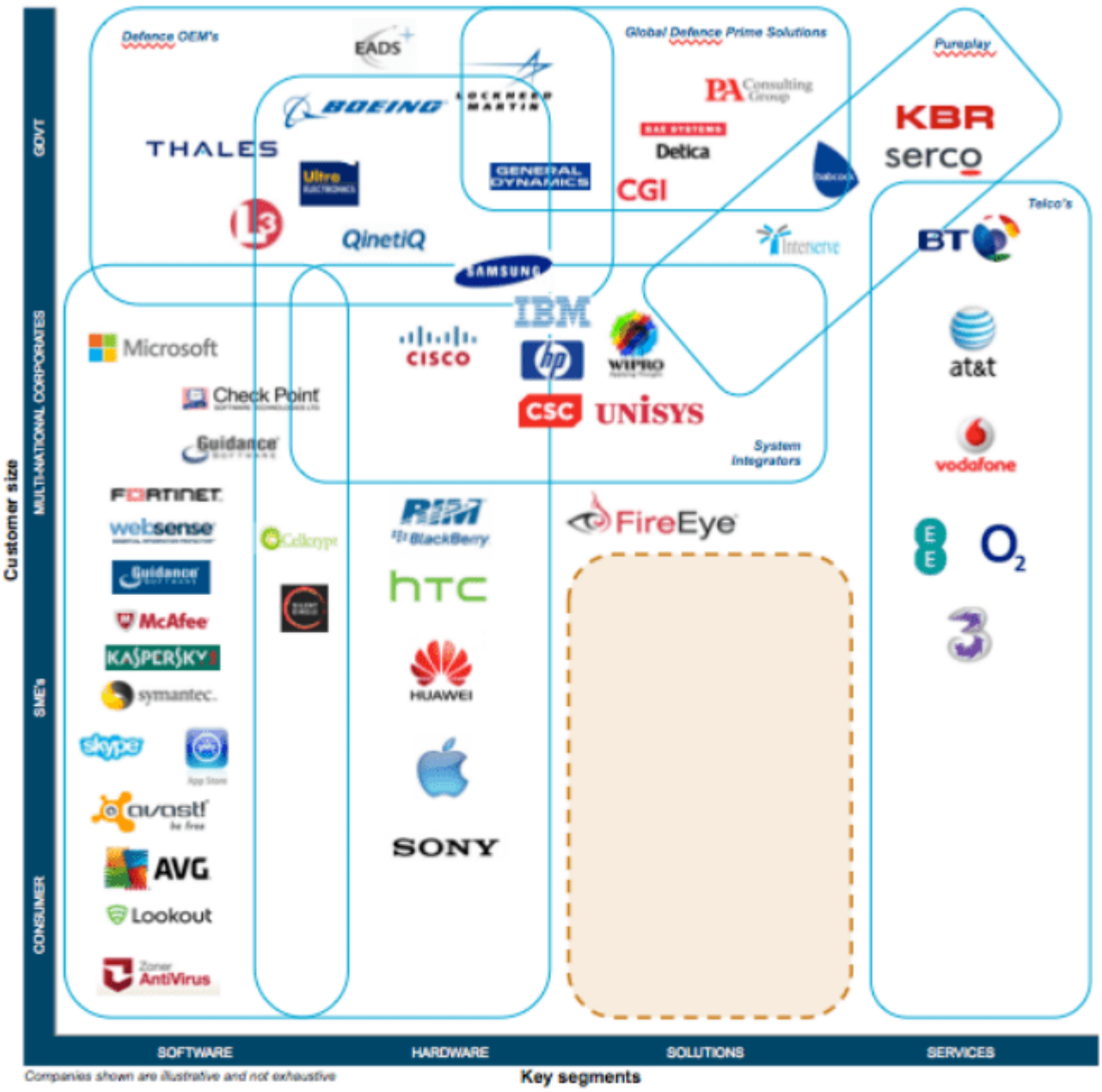


Fig 11: Defining the cyber security market and opportunity analysis.

Competition in each of the six mobile security sub-sectors is currently focused on single technology or product offerings that, due to product costs, are targeted at larger commercial organisations and inaccessible to the individual smartphone or tablet user or smaller business. Software offerings are generally limited to basic anti-virus and anti-malware apps.

The leading technical expertise in this sector is found in the UK and US. Much of the technical know-how, innovation and product development in the sector to date has been driven by individuals with experience from the Government, military or leading defence or technology primes. Applying this expertise towards the individual consumer or small business, and doing so in an easily comprehensible and affordable manner, is key, since the defence primes cannot do so organically given their high cost base and required economies of scale.

A relatively small investment (even as small as circa sub £15 million) would enable an investor critical exposure to this sector and enable the acquisition of a revenue producing company that could be used as a platform to grow organically and as a consolidator of further technologies, expertise and businesses.

Eisvogel have identified a number of potential target companies in both the UK and US that have developed technologies specifically for the mobile device security market. Project Aspen is the name given to a targeted investment strategy to acquire a UK based provider of encrypted voice, data and video and mobile data security services and use as a platform to acquire and grow a leading consumer and SME focused mobile device security solutions business. Eisvogel has identified a number of further bolt-on expertise, technology and businesses to enable the development of a single integrated global mobile security solutions business.

The US government is currently investing in secure mobile voice capability for government departments and agency customers, through companies such as L-3 Communications and General Dynamics. We know that the US Government is working with General Dynamics and Samsung to create a secure mobile capability based on consumer technology, but again purely for official US Government use. The UK government has long wrestled with its own secure voice strategy, but has so far failed to reach a definitive solution, not wishing to back the wrong horse. Instead, UK is relying in part on US technology through e.g. the General Dynamics Sectera product set, and slowly licensing other products that are of a sufficient quality level for the lower end government users e.g. Cellcrypt.

As a stop gap measure, many corporations are relying on 'Good' technology, amongst others, to create a trusted enclave within a portable device to access corporate email or other resources on a tablet or smart phone, allied with two factor authentication (for example RSA). While these approaches are satisfying a need in the short term, they only answer part of the question, create more overhead in terms of IT systems management, and alienate the user due to lack of whole device/cross-application integration and the ever growing number of unique passwords and PIN numbers that have to be generated, managed and remembered.

Meanwhile the normal consumer gets by with whatever is available, vaguely aware and uncomfortable of the risks and the lack of security that appears to be 'out there'. False comfort is provided by, for example, the banks who reimburse for losses incurred rather than improve their defences, citing cost and user unacceptability as reasons to do little. Conversely, mobile operators are being less forgiving, refusing to reimburse users who have lost their devices and had large bills run up in their name by criminals.

There is therefore a growing atmosphere of concern and disquiet about security in the mobile environment which needs satisfaction.

There are a number of enterprises that seek to fill the important mobile security market gap. They generally divide into two areas: companies that focus on the anti-virus side of security, protecting the device; and those that focus on the traffic - encryption mainly, at the device, data and network layers. The anti-virus providers are usually offshoots of the big players; the voice security community range from hardware engineers, through system on chip designers to software encryption and secure mobile virtual network operators: i.e. from device specific capability to 'secure' private networks running over existing bearers.

None of these firms has a monopoly in the market. The bigger players include Rohde & Schwarz TopSecure, to the mid-size including Cellcrypt (owned by Porton Capital); Koolspan (Security Growth Partners, TWJ Capital, Rose Tech Ventures); Lookout (Accel Partners, Andreessen Horowitz, Index Ventures, Iris Capital, Khosla Ventures and Trilogy Equity Partners); SilentCircle (US); Golden Orb GO Secure (Waterbridge); Celltrust (own management); Kryptos (India); Sirran (UK/Ireland); X-Reach (own management). Few of these firms provide the integrated end-to-end solutions that will be necessary across mobile platforms. The goal is delivering a great user experience while maintaining a fast and robust security infrastructure and leveraging the power of the cloud for advanced detection, analysis and updates.

At the smaller company scale (e.g. Sirran, Celltrust, X-Reach) the technologies already in the market place offer innovative and robust technically proficient products that are well-suited consumer use. The issues are that they lack critical corporate scale, generally have inexperienced management, limited routes to market and insufficient capital to develop their products and businesses to the next stage of maturity. In addition,

their distribution and after-sales support mechanisms are often immature, creating larger delivery risks through the sudden 'big contract failure' syndrome. In the main their funding needs are not large, but their ability to access capital is limited, and they need this finance to leverage good capability to grow in a large global market. These companies represent to us the key opportunities through which to gain the most effective investment exposure to this market.

There are a number of companies that we have already identified and are engaged with in the UK that provide good examples of this kind of target business. Strong technology, gaining market traction with key customers, and high quality contract wins already to their credit. They need capital and management resources and are ideal candidates for effective growth capital investment combined with strategic and business development support. There are also a number of these companies which could then form the basis of a series of further bolt-on acquisitions to provide further product and service expansion and to provide wider IT integration capabilities. The ultimate exit targeted would be expected to be to one of the larger UK/US defence primes once sufficient scale and IP had been built. The acquisition attraction to the primes is the inability and inefficiency for them to grow these dynamic and niche capabilities organically (for example the rationale behind BAE's acquisition of Detica).

We now live in a world with billions of connected devices. Mobile is rapidly becoming the dominant computing platform and as users do more with these devices, security is essential to keep them effective and safe. Protecting those devices and the data they contain from the growing threats facing mobile users today is critical. Eisvogel is actively targeting investment and partnering opportunities with companies that build security software that protects people, businesses and networks from mobile threats and are scalable with the support of effective growth capital.

Authors biographies

Robert Bassett Cross – Managing Partner Eisvogel Capital LLP. Robert is a former investment banker at J.P. Morgan, where he was a member of the UK Corporate Finance team, advising clients from a number of sectors, with a particular focus on the oil & gas, mining, and aerospace & defence sectors on general corporate advisory, equity capital markets and M&A transactions. During his time at J.P. Morgan, Robert was involved in over $20 billion worth of transactions across the spectrum of advisory and offerings roles. Robert's defence technology sector clients included BAE Systems, QinetiQ and Ultra Electronics. Prior to his career in investment banking, Robert was a British Army Special Forces officer who was widely respected as the leading military officer of his generation and fulfilled some of UK defence's most demanding and sensitive appointments during the last decade as a commander on combat operations in Iraq, Afghanistan and elsewhere around the globe. Robert was awarded the Military Cross for bravery and leadership on combat operations in Iraq. Prior to leaving the Army Robert was in charge of equipment procurement and future capability development for UK Special Forces and developed close relationships with companies from the aerospace & defence, industrial technology, and security sectors across Europe and North America. Robert was one of the early leaders behind the development of military application of electronic targeting and cyber warfare techniques on combat operations and helped design many of the tactics, techniques and procedures in these fields now employed by the UK military. Robert graduated from Exeter University with a bachelors degree in law (LLB (Hons)).

Ben Collins – Founder Aptus Technology. Ben is a former US Special Operations Officer and following his military service founded and led a data analytics company, Aptus Technologies. The concept behind Aptus was to deliver an autonomous capability to analyze and find relationships within the large unstructured data sets that was overwhelming the military intelligence analysts in Afghanistan and Iraq. Ben led the company through initial concept and funding to its first customers and growth into the UK market. Ben was instrumental in developing the network and strategy for initial take up and acquisition strategies in the defense and intelligence community marketplace. Upon securing one of Aptus' core customers, Boeing Defense in the United Kingdom, Ben traveled to the UK and led the UK entity to achieve $1M in revenues in the first year of operations. In developing the engagement strategies for both markets, Ben identified and helped build one of the first mobile platform applications tested for tactical environment. Prior to founding Aptus Ben served for 6 years in the US Special Forces. In 2001, Ben was assigned to Special Operations Command and deployed for Operation Iraqi Freedom in Iraq and Enduring Freedom in Afghanistan. After eighteen months of training and language school to learn Arabic, Ben earned his Green Beret and took command of a Special Forces Detachment and deployed on combat operations in Afghanistan where he was awarded the Army Commendation for Valor for his actions in combat. Completing multiple combat rotations in support of the Global War on Terror, Ben concluded his Army service as an Operations Officer for a Special Forces Battalion, managing all the daily combat operations and providing detailed mission and contingency planning for over 150 Special Forces Soldiers. Ben attended the George Washington University, in Washington, D.C.

William Egerton – CEO Egerton Advisory and Former Strategy Director General Dynamics UK

Bill is a strategist in defence and security, with a deep knowledge of information and cyber security. His roles have included working closely with the UK Government on the national information assurance and cyber security strategies, including the national debate around securing voice traffic. He has advised government and civilian entities on the management of sensitive information through change; advising governments on the implications for them and their supply base of the changes in technology and acquisition model; developing corporate market entry strategies for defence primes seeking to enter adjacent security markets; and ran a security start up delivering close protection support and physical asset protection to US contractors supporting reconstruction in Iraq. Prior to this Bill was a diplomat with the UK's Foreign Office serving in Moscow and New York. Bill holds a Bachelors Degree from Cambridge University in Modern Languages, and an MBA from Imperial College Business School in London. He speaks French, Spanish, and Russian, holds the highest security clearance, and continues to be actively involved in cyber security and information risk management.

Recent notable attacks

2007 - Retail giant TJX was hacked and 45 million customer records, including names and credit card data, were stolen by cyber criminals.

Cost: >$250m

2008 - Hackers breached networks at Royal Bank of Scotland's WorldPay, allowing them to clone 100 ATM cards and withdraw cash from machines in 49 cities.

Cost: >$10m

2008 - Marathon Oil, ExxonMobil, and ConocoPhillips were hacked and lost data detailing the quantity, value, and location of oil discoveries around the world.

Cost: >$15m

2011 - Cybercriminals penetrated the PlayStation network. Personal information for more than 80 million users was compromised.

Cost: >$170m

2011 - Citibank reported that credit card data for 360,000 of its customers were exfiltrated using a relatively simple manipulation of URLs.

Cost: >$3m

2012 - A hacker group linked to Iran launched a targeted and sustained denial-of-service attack on US bank websites.

Cost: >$100m

2012 - Worldwide cyber-attack, operating since at least 2007, discovered. Hackers gathered information through vulnerabilities in Microsoft's Word and Excel programs.

>7 Terrabytes stolen

FTSE 100 Co – Name not disclosed

2012 - The head of the UK Security Service stated that a London-listed company lost an estimated £800m ($1.2 billion) as a result of targeted cyber attacks.

Cost: c.$1.2bn

2013 - The New York Times, Wall Street Journal, Washington Post, Bloomberg News reveal that they had been the victims of persistent cyber attacks, originating from China.

2013 - Der Spiegel reveals that EADS and German steelmaker ThyssenKrupp recorded major attacks by Chinese hackers.

2013 – Banks websites targeted in denial of service attacks, preventing customers accessing online accounts.

2013 - Burger King's Twitter account hacked and logo replaced with a McDonalds logo.

2013 - J.P. Morgan Chase's website was attacked and left inaccessible to customers for 24 hours and NBC.com's website was defaced by hackers.

2013 - Online ticketing service Vendini announced that a cyber intruder had gained access to information about 1 million accounts.

Cost: >$5m

2013 - Grocery store chain Schnucks announced that 2.4 million customers had their credit card numbers compromised during a four-month cyber breach.

Cost: c.$80m

2013 – Facebook alerted users of a security breach that exposed contact information of 6 million users.

2013 – 22 million Yahoo! Japan's user IDs may have stolen during an unauthorized attempt to access the administrative system

2013 – Financial Times was hacked in a phishing attack on the company's email accounts by supporters of the Syrian Electronic Army

2013 – A gang of cybercriminals in 26 countries stole $45 million by hacking into a database of prepaid debit cards.

Cost: >$40m

2013 – Anglo American had its internal databases hacked and dumped online revealing personal details of investors and shareholders.

2013 - Data breach at Epsilon, marketing and handling services firm to JP Morgan Chase, Best Buy, and other major financial services, retailers and other major companies

Cost: $225m - $4bn

2013 – Hackers comprised database of Living Social, an Amazon owned corporation, and obtained personal information of 50 million users.

2013 – Evernote suffered a security breach that resulting in the company issuing a password reset to all 50 million users.

2013 - The New York Times, Wall Street Journal, Washington Post, Bloomberg News reveal that they had been the victims of persistent cyber attacks, originating from China.

2013 – An extremely sophisticated attached accessed personal data of 250,000 users. Resulting in extreme reputational damage.

References:

1. PWC & BIS Information Security Breaches Survey 2013 Technical Report.
2. PWC Cyber Security M&A Review November 2011.
3. PWC & Technology Safety Board Information Security 2020 Report.
4. Gartner Forecast Overview: Security Infrastructure 2010-2016, 2Q12 Update.
5. Frost & Sullivan Cyber Security – From Luxury to Necessity, February 2011.
6. UK Federation of Small Businesses Cyber Crime Survey Report, May 2013.
7. Cloud Security Alliance Data Security and Privacy Challenges Report, November 2012.
8. Verizon Report Data Breach Investigations Report 2013.
9. Norton Cyber Crime Report 2012.

About Eisvogel Capital LLP

Eisvogel is a London based investment firm that invests growth and development capital in private UK and European high-tech industrial and manufacturing businesses. Eisvogel was founded in 2012. Eisvogel has particular expertise in the aerospace & defence, cyber and security technologies sectors.

Contact details

EISVOGEL CAPITAL LLP

7 OLD PARK LANE

LONDON W1K 1QR

+44 203 651 3434

info@eisvogelcapital.com

www.eisvogelcapital.com