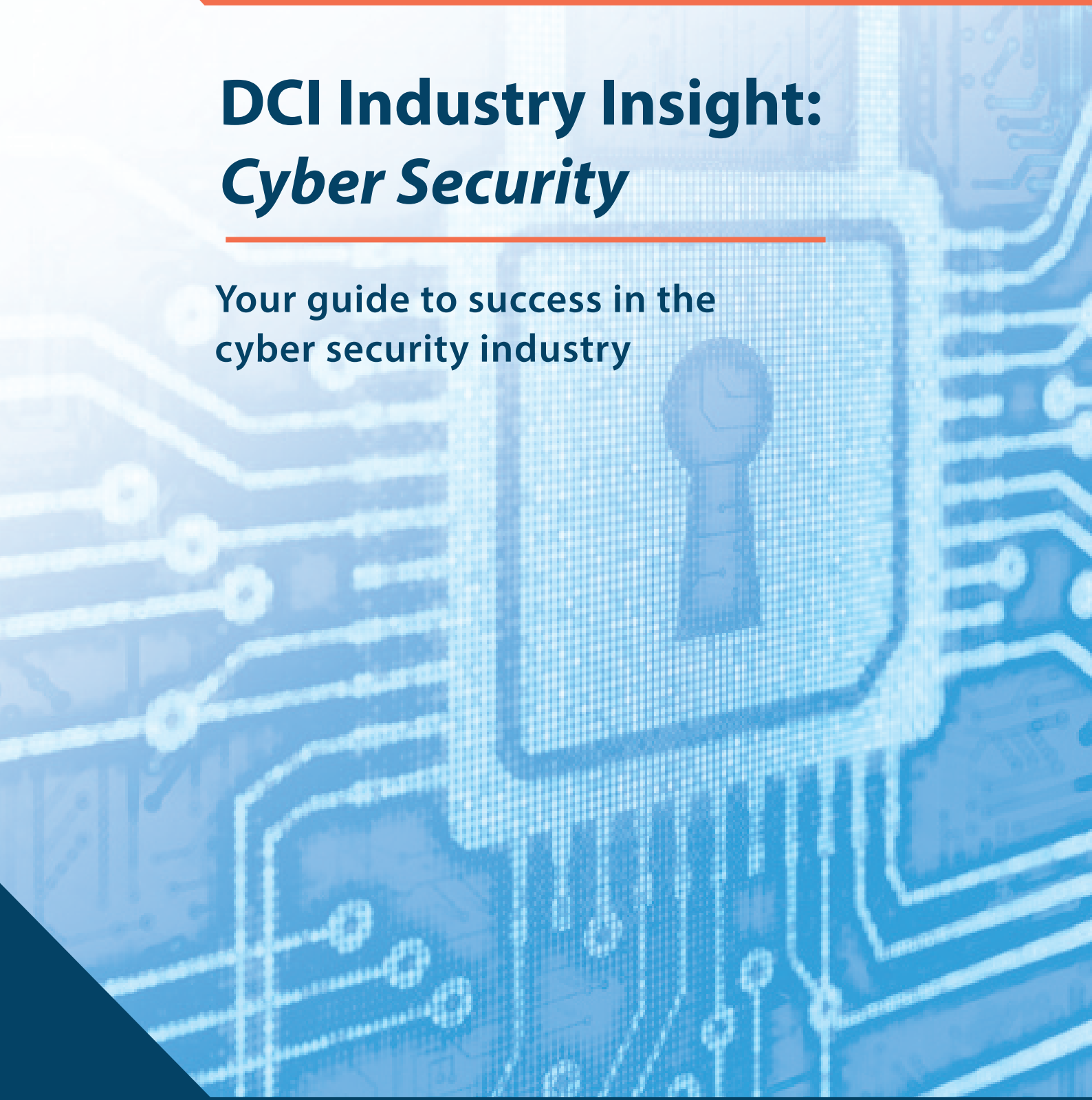
DCI DEFENCE CONTRACTS INTERNATIONAL

Delivering Precision Intelligence

DCI Industry Insight: *Cyber Security*

Your guide to success in the cyber security industry



www.dcicontracts.com 0845 270 7092

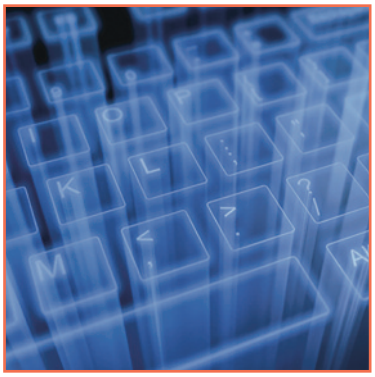
DCI Industry Insight: Cyber security

By *Michael Crosby*
Defence Contracts International Communications Officer
Follow DCI on Twitter
@DCItenders
Connect on LinkedIn
Michael Crosby: *uk.linkedin.com/in/michaelcrosby2/*

Defence Procurement Intelligence:
https://www.linkedin.com/groups?mostRecent=&gid=4967697&trk=my_groups-tile-flipgrp

Table of Contents

04	Introduction
05	Part one: Security for your business
08	Part two: The cyber market
10	Part three: Future threats and opportunities
13	Defence Contracts International

Introduction

We live in the information age.

The internet revolution has made us more connected than ever before, and we have come to rely every day on technologies which were in their infancy just a few years ago.

From smart phones and social media to 'chip and pin' and cloud computing, cyber technology is a fundamental part of daily life, bringing with it both massive challenges and massive opportunities for companies of all sizes.

The global cyber security market is expected to grow at an annual rate of 11.8% over the period to 2018[1].

In order to maintain a commercial advantage, it is important for businesses to protect themselves from cyber threats including hacking and system failure, as well as understanding how to transform these threats into business opportunities in areas such as training, IT, data protection and emergency planning.

This *DCI Industry Insight: Cyber security* report aims to provide you with an overview of this highly lucrative sector, showing current trends in the market, identifying potential growth areas and detailing the importance of remaining compliant with the latest cyber security protocols.

Part one: Security for your business

A recent report by the World Economic Forum looked at the top ten global trends affecting the world. Number four on the list[2], for the first time, was 'intensifying cyber threats', which came just behind tensions in the Middle East, income disparity and global unemployment in terms of worldwide importance.

As we turn increasingly to cyber technology to conduct our daily lives and business interests, we invariably open ourselves up to a whole new generation of dangers. As cloud computing connects more and more devices to a shared network, terrorists, hackers and opportunists have even more opportunity to disrupt our lives.

According to the Department for Business, Innovation and Skills, 93% of large corporations and 87% of small businesses have reported a cyber security breach, with the average cost of a single breach estimated as between £450,000 and £850,000[3].

It is anticipated that, by 2020, governments and enterprises will leave 75% of sensitive data unprotected, and some estimate that failure to implement cyber security solutions could cost the world economy $3 trillion between now and 2020[4].

In 2013, the world was hit by the largest cyber fraud in history after 160 million credit cards were compromised in the US, causing damage worth an estimated $300m[5].

In an attempt to promote safe and secure online practices and to avoid this potential global cyber threat, governments around the world are looking more and more at the issue of cyber security, how it can be implemented and, in some cases, how it can be made a mandatory pre-requisite before the award of any government contract.

1 CNBC, *Research and Markets: Global Cyber Security Market Report 2014-2018,* http://www.cnbc.com/id/101710980

2 CSO, *Cyber threats makes it to number 4 on the Global WEF Agenda,* http://www.cso.com.au/article/548110/cyber_threats_makes_it_number_4_global_wef_agenda/

3 Department for Business Innovation and Skills, *Information Security Breaches Survey, Technical Report*, 2013

4 CSO

5 ibid

Digital by Default

From April 2014, the Government Digital Strategy committed the UK Government to pursuing a 'digital only' approach to its processes.

The strategy outlines a potential £1.8bn saving each year[6] by moving to online only services, aims to streamline processes and will be a requirement for all departments in coming years.

The first main stage of this new approach was the launch of the GOV.UK website, where services from 34 government departments and 331 agency and public body websites have been merged into one, with the aim of making these digital services so easy to use that it is the preferred way of accessing them.

Cabinet Office Minister Francis Maude made the Government's digital agenda clear:

> *"A little over a year ago this Government set out an ICT strategy focused on making Government technology cheaper, more transparent, more innovative and flexible – with more opportunities for new suppliers, including SMEs.*
>
> *"Digital is not just another channel; it is the delivery choice for this generation.[7]"*

The UK's position is being used as a model overseas. A recent report by the Commission of Audit has recommended that Australia adopt the UK's 'digital by default' strategy as well as a 'cloud first' strategy for government IT[8] .

As government looks to move functionality further online, it has never been more important for firms to establish themselves not only as an online presence, but also as an enterprise with safe and secure online processes.

[6] GOV.UK, *Digital by Default Service Standard,* https://www.gov.uk/service-manual/digital-by-default

[7] Supply National SME Engagement Programme, *Maude aims for Digital by Default,* https://www.supplycontracts.co.uk/news/maude-aims-for-digital-by-default/

[8] The Register, *Australia told to follow UK's 'Digital by default' strategy,* http://www.theregister.co.uk/2014/05/01/australia_told_to_follow_uks_digital_by_default_strategy/

Cyber essentials

In the UK, the Government has introduced the Cyber Essentials scheme, a certification programme awarded to organisations which exhibit secure and protected cyber processes.

Crucially, the UK Government will make this certificate a mandatory requirement for organisations bidding for certain contracts deemed 'high risk'. These are likely to include contracts for ICT, defence and those dealing with sensitive personal information.

In light of this, the UK Government unveiled 10 Steps to Cyber Security[9], which have been published to help businesses remain compliant and qualify for the Cyber Essentials credential.

The ten steps are as follows:

- Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline build to all devices. Protect data both in transit and at rest
- Produce user security policies covering acceptable and secure use of the organisation's sys-tems. Establish a staff training programme. Maintain user awareness of the cyber risks
- Establish an incident response and disaster recovery capability. Produce and test incident management plans. Provide specialist training to the incident management team. Report criminal incidents to law enforcement
- Establish an effective governance structure and determine your risk appetite. Maintain the Board's engagement with the cyber risk. Produce supporting information risk management policies
- Establish account management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs
- Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing on to corporate system
- Establish a monitoring strategy and produce supporting policies. Continuously monitor all ICT systems and networks. Analyse logs for unusual activate that could indicate an attack
- Apply security patches and ensure that the secure configuration of all ICT systems is main-tained. Create a system inventory and define a baseline build for all ICT devices
- Produce relevant policy and establish anti-malware defences that are applicable and relevant to all business areas. Scan for malware across the organisation.
- Protect your networks against external and internal attacks. Manage the network perimeter. Filter out unauthorised access and malicious content. Monitor and test security controls

Establishing your organisation as having a safe online presence can be a real selling point to your customers and to potential public sector clients, particularly as government seeks to make cyber security a mandatory requirement before the award of certain contract opportunities.

---

[9] GOV.UK, *10 Steps to Cyber Security,* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/73128/12-1120-10-steps-to-cyber-security-executive.pdf

Part two: The cyber market

The cyber market is one which has been largely unaffected by the continuing global economic downturn, with steady growth recorded across sectors worldwide.

Global market drivers

The growth in the cyber security market being exhibited across the globe is being driven by a number of factors, including:

- Increasing number of cyber threats
- Greater vulnerabilities as we move further towards cloud computing, mobile and social media
- The need to increase awareness of potential threats
- Technological advancement driving product and service innovation
- Increasing regulation, particularly around the need for increasingly secure personal data

Taken together, these drivers are creating a varied marketplace with growing opportunities for organisations of all sizes to enter the supply chain.

Worldwide marketplace

Global cyber security spending was $60bn in 2011[10]. In 2014, it has grown to $95.6bn and, by 2019, the cyber security market is expected to be worth $155.74bn – a Compound Annual Growth Rate of 10.3% from 2014 to 2019[11].

The global cyber security market is currently dominated by North America, with the US being the largest defence spender in the world. Overall, North America is set to spend $93.6bn on cyber security during the next decade. As the US looks to remove more and more of its defence activity out of the Middle East, the Government has announced reductions in tanks and other major weapons programmes, diverting its spending towards IT and cyber security programmes.

Europe represents the world's second-largest cyber market, currently valued at around $24.7bn. The Asia-Pacific region is projected to spend an estimated $23.2bn on cyber security during the next ten years, followed by the Middle East and Latin America with $22.8bn and $1.6bn respectively[12].

Countries in the Middle East, Asia Pacific and Latin America are also expected to ramp up spending on cyber security during the forecast period.

[10] PricewaterhouseCoopers, *Cyber Security M&A: Decoding deals in the global Cyber Security industry,* http://www.pwc.com/en_GX/gx/aerospace-defence/pdf/cyber-security-mergers-acquisitions.pdf

[11] Markets and Markets, *Cyber Security Market worth $155.74 Billion by 2019,* http://www.marketsandmarkets.com/PressReleases/cyber-security.asp-

[12] Market Watch, *The Global Cyber Security Market 2013-2023,* http://www.marketwatch.com/story/the-global-cybersecurity-market-2013-2023-2013-06-17

USA

In terms of defence, the US Budget remained unchanged for 2015 at $496bn. However, although the total defence spending in the Budget has been largely unchanged since last year, the most recent Budget does reveal important shifts in priorities with a move away from spending on the conventional Armed Forces and greater investment in cyber security.

The spending plan President Obama sent to Congress is set to shrink the size of the US Army from 490,000 active-duty soldiers to 450,000, the smallest force since before World War II.

The move is in line with withdrawal from Iraq and declining activity in Afghanistan as the country moves towards a 'post-war' mindset, with less reliance on troops on the ground and greater focus on technology and cyber defence.

The Budget included a cyber security request amounting to more than 1 per cent of the total Pentagon request.

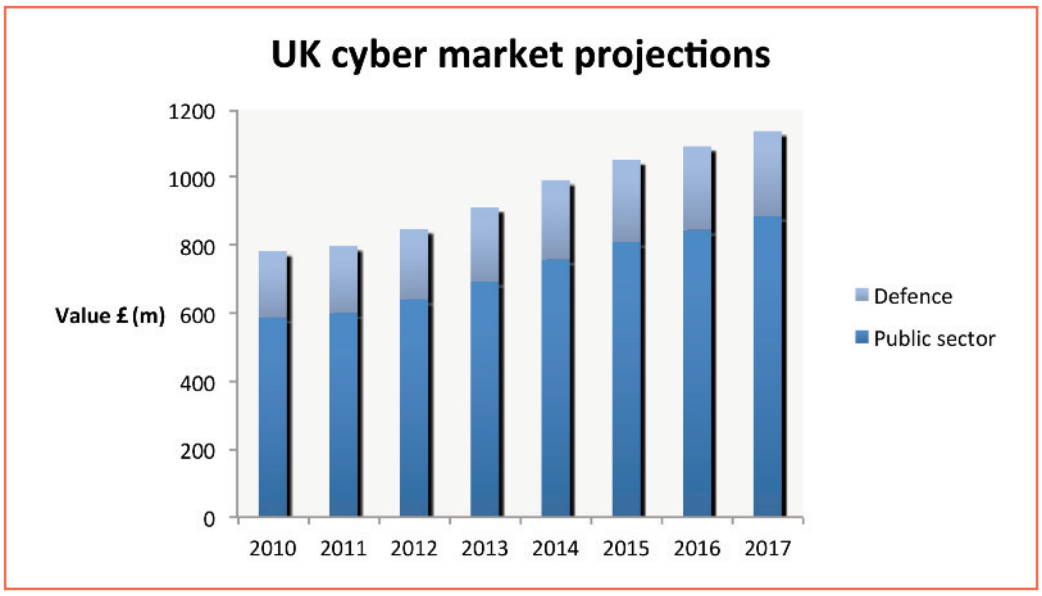
Defense Secretary Chuck Hagel said of the decision to reduce the size of the Army: *"We chose further reductions in troop strength and force structure in every military service – active and reserve – in order to sustain our readiness and technological superiority and to protect critical capabilities."*

The Budget will boost funding for the Comprehensive National Cybersecurity Initiative, which aims to create a front line of defence against network intrusion and hacking.

UK

In 2010, the UK Government made cyber security a 'Tier 1' threat priority and allocated £650m for various cyber security initiatives in its 2010 National Security Strategy[13].

In addition, the projected market growth for cyber security across the UK demonstrates the value this sector is likely to have for private companies in the next few years[14]:



[13] Francis Maude, *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world,* November 2011

[14] Statista, *UK cyber security market size,* http://www.statista.com/statistics/289157/uk-cyber-security-defence-and-intelligence-sub-segment-size/

UK continued...

In order to secure the vast economic and social benefits that cyber can offer the UK, a new approach to cyber security has been unveiled by Government. Its 2015 objectives are as follows[15]:

- For the UK to tackle cyber crime and be one of the most secure places in the world to do business
- To be more resilient to cyber attacks and better able to protect our interests
- To help shape an open, stable and vibrant cyberspace which the public can use safely
- For the UK to have the cross-cutting knowledge, skills and capacity it needs to underpin its cyber objectives.

Part of the Government's plan to achieve these goals includes a programme of partnership between the private enterprises, the public sector and law enforcement to share information and resources, respond to common challenges and actively deter threats.

Examples of this work in action include the Defence Cyber Protection Partnership, which aims to increase awareness of cyber risks by sharing threat intelligence, and the British Security Industry Association, the trade association for the professional security industry in the UK.

Part three: Future threats and opportunities

The scale of our current dependence on cyber technology puts huge pressures on our infrastructure, our workplace and our homes.

In addition, the rise of new threats means the industry is constantly evolving, and your business processes and attitudes must evolve with it. Predicting and understanding how the industry is set to change can set your business apart from your competitors.

New threats

Social media is one of the world's fastest growing phenomena, with most individuals and businesses now having some form of presence on various social media platforms including Facebook, Twitter, LinkedIn or Google+.

The popularity of these sites inevitably brings with it threats to businesses which were not present even ten years ago. Business-critical information can now enter the public domain more quickly than ever at the press of a button, reaching audiences at a rate that can be difficult, if not impossible to manage.

For example, a fake tweet by an individual impersonating a Russian interior minister caused crude oil prices to rise by over $1 a barrel before traders realised the news was false[16].

However, companies which recognise the value of social media have demonstrated that success can be achieved through empowering staff to communicate sensibly via social channels on behalf of the business.

[15] ibid

[16] Computer Weekly, *Social media: A security challenge and opportunity,* http://www.computerweekly.com/feature/Social-media-a-security-challenge-and-opportunity

Analysis of information in social conversations can produce security intelligence to improve security processes and enhance performance, can create marketing and advertising channels and can help personalise your organisation to potential customers.

By handling social media effectively, an organisation can harness the power of these platforms while minimising risks by implementing a comprehensive policy backed up with training.

Politically motivated attacks via social media via so-called 'hacktivists' are also causing real concern for government departments and real opportunity for the security industry.

HM Government reported that 60% of organisations are implementing activity to develop cyber security skills within their organisation, with this number only set to rise as technology continues to develop. For organisations which can train, supply or inform cyber security processes, the future is brighter than ever.

Other potential market drivers

Growth in the cyber security industry is expected to maintain pace for the next decade, and experts predict that this growth will be driven by the following market developments:

Infrastructure revolution

As computing resources become more centralised and adoption of cloud computing becomes widespread, the split between work and personal life becomes blurred. This trend is likely to continue, resulting in the evolution of user interfaces, the emergence of new technologies such as 'wearable tech' and greater integration of devices.

Data explosion

With more people connected via the internet, the world is essentially becoming a smaller place. As visual data and video becomes more common, greater traffic is to be expected, with the accompanying need for faster connection speeds and the need for greater classification of data. There is to be increasingly seamless connectivity between devices as people begin to move more information online and as businesses and governments move to 'digital by default'.

Future finance

Analysts are predicting the continued proliferation of digital finance such as bitcoin, which uses peer to peer technology without the need for centralised banks. Whether this development continues to gather pace remains to be seen, but the rise of electronic banking is certainly set to go unchallenged.

Tougher regulation and standards

The issue of net neutrality is already coming to the forefront of the cyber industry. In the US, a recent decision to overturn the Open Internet Order, which aimed to ensure that the internet was an open, free and shared space, has been met with severe criticism. Pro-net neutrality activists state that overturning this order allows multi-speed internet 'lanes', with the wealthy and big businesses paying more for increased internet freedom, effectively freezing out individuals and smaller firms which do not have the money to compete.

As regulations against piracy continue to evolve and with increased internet censorship in countries such as Turkey and China, the very nature of the internet could be set for a fundamental shift in coming years.

Top 5 most compromised industries[17]

1. **Retail: 45%**
2. **Food and drink: 24%**
3. **Hospitality: 9%**
4. **Financial services: 7%**
5. **Non-profit: 3%**

The industries which are most vulnerable to hackers are those which deal in large amounts of personal data, with the most common points of attack in these industries being eCommerce websites (48%) and payment processing points (47%).

As a result, these industries have the greatest need for additional cyber security protection, particularly for the personal data they hold, and present the greatest opportunities for businesses which can supply this security.

If an organisation does suffer a data breach, a number of priorities must be addressed as quickly as possible. Skills in this area are therefore likely to be amongst those in highest demand in the cyber security industry for organisations which can turn these threats into opportunities.

Where your business can be effective

Awareness

Educating employees on security processes is likely to be a growing concern among businesses and organisations of all sizes. Opportunities exist in external security consultancy, security process testing and simulation exercises. The more employees understand the risks associated with cyber technology, the more an organisation can protect itself.

User access

More users create more potential threats. Shared passwords, hot desking and temporary keycards can easily cause a brief lapse in security process, which can then be exploited. Access management is therefore critical in business, and consistent review of security processes, authentication and vendor controls are often outsourced, particularly among small businesses, creating great business opportunity for firms specialising in this area.

[17] Trustwave, *2013 Global Security Report,* http://www2.trustwave.com/rs/trustwave/images/2013-Global-Security-Report.pdf

Data protection

Understanding data is paramount to protecting it. How data is created, stored and accessed is crucial to keeping it secure. As the most common area of attack for a business is eCommerce websites and payment points, there are ample opportunities available in data management, covering the life cycle of data from creation to destruction. Implementation of firewalls, anti-malware protections and intrusion detection systems are likely to be in high demand.

Internal asset management

As working from home becomes more common in business, sharing devices across networks and consoles presents significant risk for organisations. Opportunities for businesses in this area include training in asset management and virus scanning techniques, implementation of appropriate security controls, and correct threat isolation and quarantine processes.

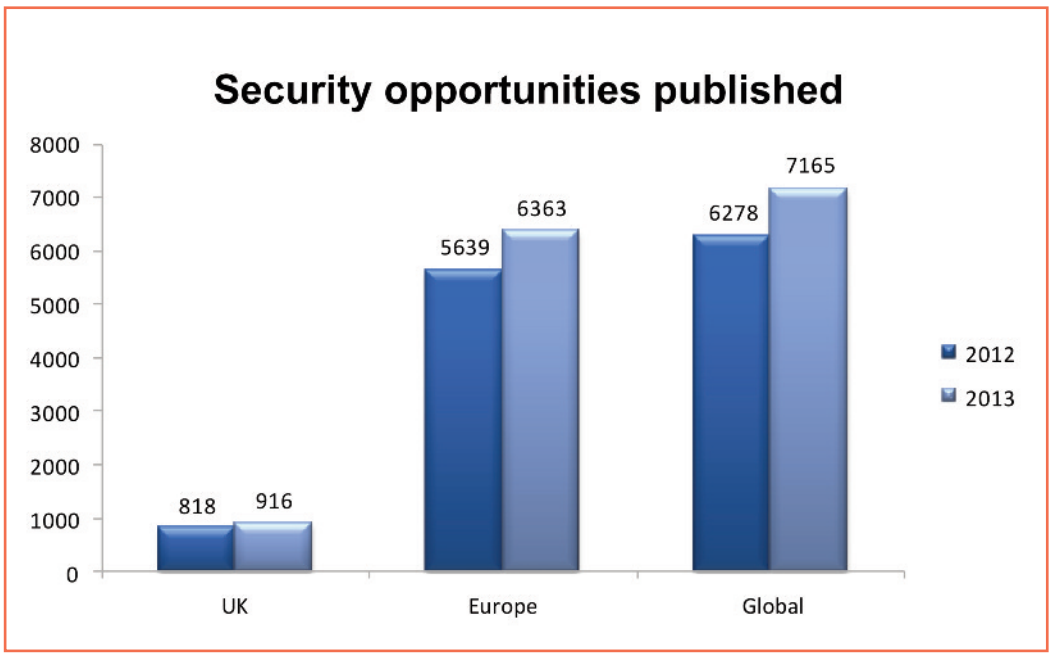
Disaster recovery

While there are obvious opportunities available in data protection, cyber security and threat prevention, it is unfortunately likely that breaches will continue to exist and cyber attacks will happen. In these cases, disaster recovery and emergency planning will be crucial to maintain business continuity, including training for key staff, incident response plans, backing up of files and networks and attack simulation exercises.

Defence Contracts International

Industry opportunity trends

The wider security market is incredibly varied, with opportunities for business of all sizes across many industries. The market has been booming in recent years and there has been a rise in the number of opportunities available to organisations such as yours that reflects the increasing value of the industry.



In total, 7165 opportunities relating to the global security industry were published in 2013, up from 6278 in 2012, representing a 14% increase in one year.

Of these 7165 opportunities, 1844 were related to the cyber sector, meaning 25% of all opportunities available in this sector had a component related to cyber security, anti-virus software and protection, firewalls, hacking and related activities.

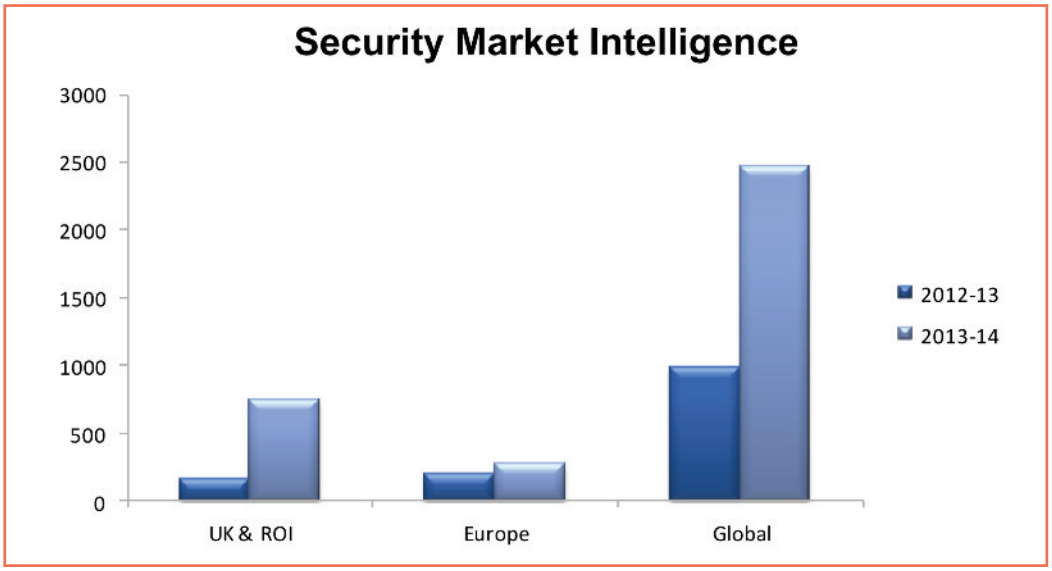
DCI has long-term relationships with the UK Ministry of Defence (MOD), the Official Journal of the European Union (OJEU) and Federal Business Opportunities (FedBizOpps). Our standing in the market means that you can have complete confidence that you'll never miss a contract with DCI, allowing you to stay competitive in this burgeoning industry.

To find out more about DCI's extensive database, visit: **http://www.dcicontracts.com/**

Market Intelligence

Understanding the trends and developments in the market which will be likely to impact upon your business can be crucial in ensuring your future success.

Market Intelligence is an innovative tool which aggregates important industry news, legislation, market developments and government announcements to provide targeted intelligence to specific business needs.



In 2013/14 alone, DCI published 6614 individual global security-related industry stories, including important news and industry announcements relating to cyber, CCTV, identification and much more.

DCI aims to help you to keep informed about all the developments in your chosen field, delivering precision intelligence to help drive your business decisions.

To find out more about Market Intelligence,
http://www.dcicontracts.com/features_marketintelligence.html

About DCI

With the cyber market booming, now is the time to ensure that your business is ready to make the most of the opportunities available.

Having visibility of the right opportunities for your business from the start is vital in gaining first-mover competitive advantage; DCI gives you more opportunities, intelligence and support than anyone else.

Our unique content and market intelligence, along with our training and events portfolio, means that DCI does more than help you find contracts – we help you win them too, supporting your business at every stage of the tender process.

Find out more at: **www.dcicontracts.com**

Next Steps:

Speak to a Business Growth Advisor
0845 270 7092

Check out the system
www.dcicontracts.com

Connect with us on Linkedin
Defence Procurement Intelligence