Supply

National SME Engagement Programme

The SME Cyber Market: How your business can benefit

The SME Cyber Market: How your business can benefit

By Michael Crosby
Supply Communications Officer

Follow us on Twitter

@SupplyContracts

Connect on LinkedIn

Michael Crosby: uk.linkedin.com/in/michaelcrosby2/

Supply: http://www.linkedin.com/groups?gid=4571375&trk=my_groups-b-grp-v

The SME Cyber Market: How your business can benefit

Contents

Introduction

In 2011, the UK Government unveiled its Cyber Security Strategy with the aim of safely and securely promoting the UK in the digital world.

The Government's aspiration is for the measures outlined in this strategy to position the UK at the forefront of the digital industry by 2015.

The Government's focus on the cyber industry presents numerous opportunities for UK small businesses. 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.

Following the publication of an update to the National Cyber Security Programme this year, it is important for small businesses to understand how to transform cyber threats into business opportunities in areas such as training, IT, data protection and emergency planning.

This report from the Supply National SME Engagement Programme aims to provide you with an overview of the business potential of this highly lucrative sector, showing current trends in the market, identifying upcoming growth areas and detailing the importance for SMEs in remaining compliant with government cyber security recommendations.

Importance of cyber security for SMEs

As we turn increasingly to cyber technology to conduct our daily lives and business interests, we inevitably open ourselves up to a whole new generation of dangers. As cloud computing connects more and more devices to a shared network, the potential for this network becoming compromised increases.

According to the Department for Business, Innovation and Skills, 87% of small businesses reported a cyber security breach in 2013, with the average cost of a single breach estimated at between £450,000 and £850,000[1].

In addition, the PricewaterhouseCoopers Information Security Breaches Report found that, among small firms, the financial impact of their worst reported attacks almost doubled between 2013 and 2014[2].

In an attempt to promote safe and secure online practices and to avoid potential cyber threats, the UK Government is looking more and more closely 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 a government contract.

Risks of online exposure

Companies must be intelligent about how they implement a cyber security policy. If not handled correctly, small businesses in particular could face real risks as their online exposure grows, and may not be able to manage cyber breaches in the same way as their larger counterparts.

The main risks facing businesses are as follows:

- Financial losses from theft of information, bank details or money
- Financial losses from disruption to trade
- Costs from cleaning affected systems and getting them up and running
- Costs of fines if personal data is lost or compromised
- Costs of losing business through damage to your reputation after a breach
- Damage to other companies in your supply chain

[1] Department for Business Innovation and Skills, *Information Security Breaches Survey, Technical Report*, 2013
[2] Update on the National Cyber Security Programme, 2014 http://www.nao.org.uk/wp-content/uploads/2015/09/Update-on-the-National-Cyber-Security-Programme.pdf

However, the cyber market is not merely one of risks to be managed, but one of massive opportunity for firms well placed to take advantage of Government focus on the cyber market in the coming years.

Online-only departments

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

The strategy outlines a potential £1.8bn saving each year[3] by moving to online-only services 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 government services.

Cabinet Office Minister Francis Maude made the Government's digital agenda clear in 2012:

"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."[4]

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

Businesses which adopt appropriate online processes will be looked upon favourably by a Government keen to build the UK's cyber profile, encourage more firms to adopt safe cyber processes and boost the UK's standing in the global cyber security marketplace.

[3] GOV.UK, '*Digital by Default Service Standard*', https://www.gov.uk/service-manual/digital-by-default
[4] Supply National SME Engagement Programme, *'Maude aims for Digital by Default'*, https://www.supplycontracts.co.uk/news/maude-aims-for-digital-by-default/

UK market

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[5].

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[6]. Expected to surpass £1bn in 2015, the public sector cyber market could grow to a value of £1.13bn within three years.

The growth in the cyber security market being exhibited across the UK is being driven by a number of global 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. In addition, the UK Government has launched a number of initiatives to boost the opportunities for small businesses in particular in this growing sector.

[5] Francis Maude, '*The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world'*, November 2011
[6] Statista, *'UK cyber security market size'*, http://www.statista.com/statistics/289157/uk-cyber-security-defence-and-intelligence-sub-segment-size/

Government steps to help

In 2014, the UK Government put the issue of cyber security at the forefront of its agenda to help SMEs both to protect themselves and to take advantage of the opportunities available in this industry.

The Government appointed Andy Williams from industry body TechUK as its first ever SME cyber 'czar' in September 2014. Mr Williams will be tasked with finding and connecting small businesses in the security field as well as promoting them at international trade events.

In addition, £4m was offered via competition for small firms looking to develop new security technology as part of a wider push to promote SMEs in the cyber market.

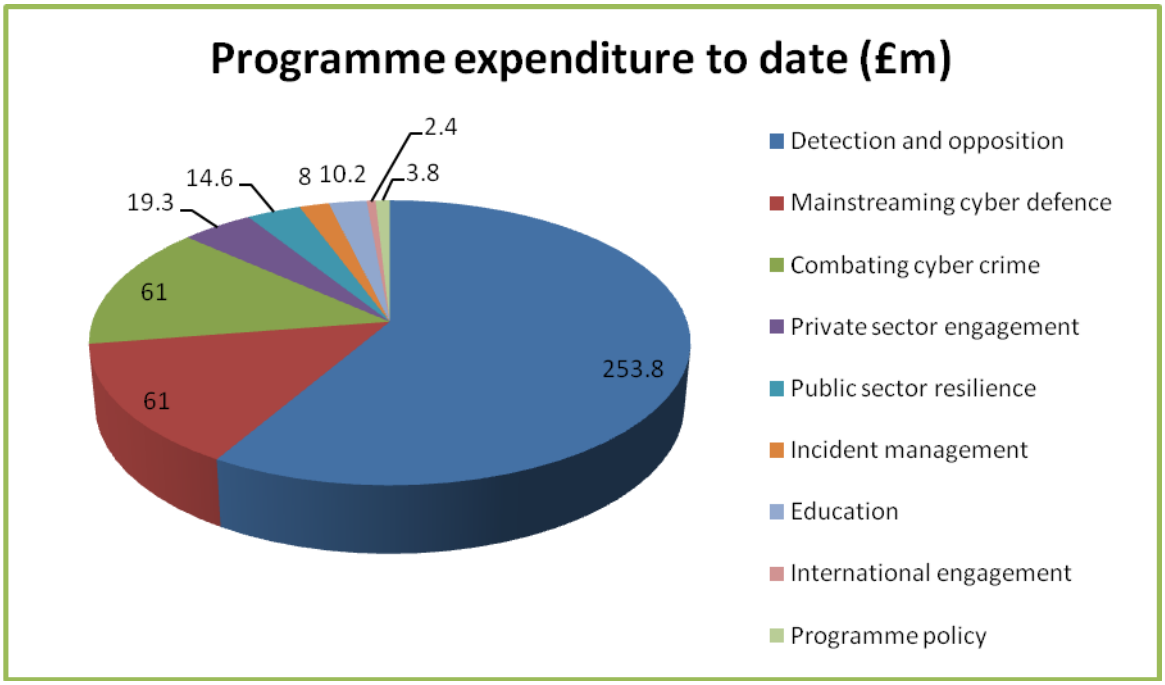
National Cyber Security Programme

The government's National Cyber Security Programme was launched in April 2011 and is expected to run until March 2016. It has a budget of £860m and sets the Government's cyber agenda for all businesses.

It has four objectives:

- To tackle cyber crime and make the United Kingdom one of the most secure places in the world to do business
- To make the UK resilient to cyber attacks and better able to protect our interests in cyberspace
- To help shape an open, vibrant and stable cyberspace which the UK general public can use safely which supports open societies
- To build the UK's cross-cutting knowledge, skills and capability to underpin all our cyber security objectives

In the three full financial years since the Programme started in 2011-12, it has spent £434.1m of the allocated £860m budget. The spend breakdown is as follows:



In 2014, the Cabinet Office ordered a review of the National Cyber Security Programme following a request from the Chair of the Committee of Public Accounts, resulting in the publication of an Update on the Programme's progress.

The Update revealed several key findings:

1) The Programme is on track, but more must be done to help SMEs

The Programme's financial management is strong and is on track to spend its budget of £860m by March 2016. However, while progress has been made in encouraging larger companies to mitigate the risks posed by the cyber industry, the Programme has thus far 'struggled to communicate guidance' to smaller firms.

2) Exports are increasing

UK cyber exports increased by 22% between 2012 and 2013. However, progress in encouraging trade and exports in cyber products and services in the UK has been slower than expected.

3) Continuing progress will be measured

The government have now agreed a methodology to measure progress against its target of £2bn of cyber-related exports, announced in 2013.

With the Programme due to end in 2016, the upcoming spending review, due at the end of 2014, together with the Strategic Defence and Security Review, will set the agenda for the cyber security market beyond the lifespan of the National Cyber Security Programme.

There is already a consensus supporting the establishment of a successor programme to build on the momentum established by the National Cyber Security Programme and to ensure that the benefits of the Programme continue to be implemented and monitored.

Cyber Essentials

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

From 1 October 2014, all suppliers must be compliant with the new Cyber Essentials controls if bidding for government contracts which involve handling of sensitive and personal information and provision of certain technical products and services.

Cyber Essentials was developed by government, in consultation with industry. It offers a sound foundation of basic 'cyber hygiene' measures which, when properly implemented, can significantly reduce a company's vulnerability. The scheme's set of critical controls is applicable to organisations of all sizes, giving protection from the most prevalent forms of threat coming from the internet.

In light of this, the UK Government unveiled *10 Steps to Cyber Security*'[7], which have been published by the Government 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

[7] 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

- Produce user security policies covering acceptable and secure use of the organisation's systems. 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 maintained. 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.

New opportunities for SMEs

Small firms in particular need to be aware of how to protect themselves from the potential risks associated with the increasing reliance on cyber operations. Larger firms may struggle to recover from a hack quickly; but due to their size a cyber hack could prove fatal to SMEs.

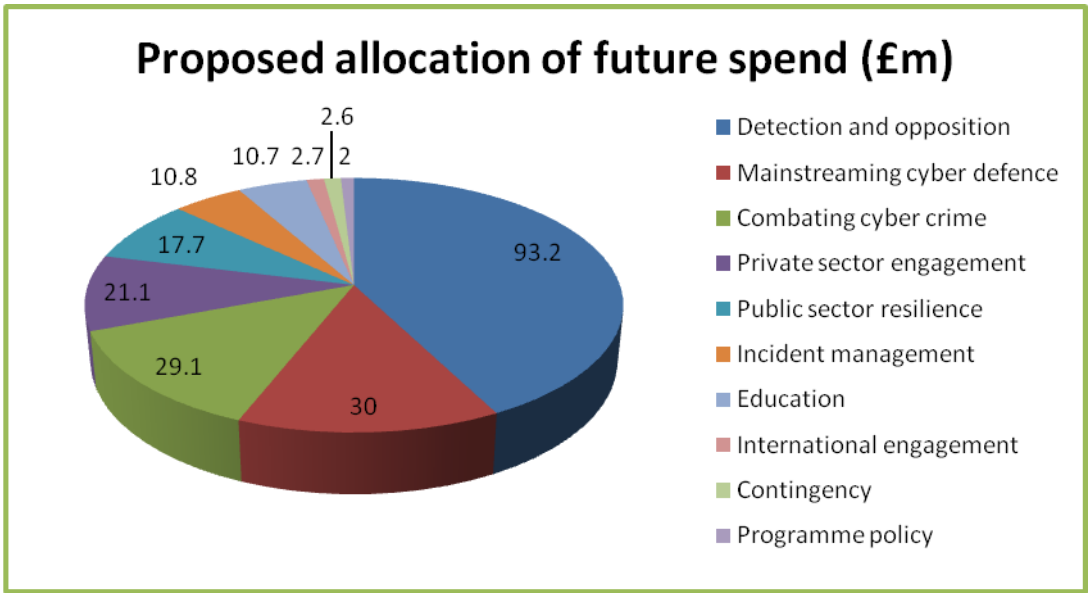
However, given the UK Government's commitment to focusing on this market in future, it would be unwise for small firms to ignore the possibilities which can also arise from the booming cyber market.

Upcoming spend in the National Cyber Security Programme

The National Cyber Security Programme is due to end in March 2016. As the scheme winds down, the final two years of the Programme's lifespan will see its highest levels of spend being allocated.

In 2014-15 (year four of the scheme), £210m is to be spent on improving the UK's security knowledge and processes, with the same figure to be allocated for 2015-16.

The spending for year four will break down as follows:



With planned spending of £93.2m, far and away the highest level of spend allocated by the Programme, the Government is placing a real focus on the country's ability to detect and defeat high-end threats, which in turn will open up huge opportunities for firms which can provide this type of security on a large scale.

There is also likely to be a greater focus on cyber security processes throughout the defence sector. As technology develops, threats to national security are becoming more likely to arise via a cyber breach than from traditional combat threats. With £30m allocated for maintaining current cyber systems, firms can expect the cyber defence market to be booming in the coming years.

Cyber Security Supplier to Government Scheme

The Cyber Growth Partnership was established to support the growth of the UK cyber security industry. It aims to encourage more suppliers to become involved in this growing market by allowing forms to advertise that they are a trusted supplier of cyber services to Government.

The scheme will allow companies to:

- Advertise that they supply a cyber security product or service to Government
- Use the Government logo in marketing collateral
- Advertise themselves on a public list of cyber suppliers to Government

The scheme is open to all companies which currently have a contract for the supply of goods and services to Central Government. Wider public sector bodies, including NHS and local authorities, are excluded from the scheme.

This should not be considered an official accreditation scheme, however, since the Government's clearance of a company is not a direct recommendation or endorsement of quality, but merely indicates that the firm has met the criteria to be awarded the contract.

The scheme runs concurrently with the National Cyber Security Programme and ends alongside it in March 2016. For further information on the scheme, email: cybersecurity@bis.gsi.gov.uk

Further opportunity for SMEs

To encourage more SMEs to protect their businesses from cyber security threats and prepare for the opportunities of this growing sector, UK Government launched 'Innovation Vouchers for Cyber Security'.

The vouchers, worth up to £5000, are specifically aimed at small firms and early stage start-ups which see value in protecting and growing their online business by having effective cyber security.

The funding will enable SMEs to secure specialist consulting and will help:

- Businesses looking to protect new inventions and business processes
- Businesses looking to 'cyber audit' their existing processes
- Businesses looking to move online and develop a technology strategy
- Business start-ups looking to develop an idea into a working prototype and needing to build cyber security into the business from the very beginning

For more information on Innovation Vouchers, visit:
https://vouchers.innovateuk.org/cyber-security

How Supply can help

For businesses such as yours, it is important to make the most of rising confidence in the public sector procurement market and the Government's increased focus on helping SMEs grow their business.

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

The Supply National SME Engagement Programme provides a key route to finding new public sector contracts and awards information.

There's a Supply subscription that's right for your business – whether you are a sole trader, a micro business or a small or medium sized enterprise. You can also choose from 'low value' or 'low and high value' subscriptions to suit your needs.

The Supply National SME Engagement Programme is your partner throughout the process of winning government contracts. We published over 58,000 UK contract notices in 2013 alone, making it the clear choice to help you grow your business in the public sector.

Win more Government business with the Supply National SME Engagement Programme