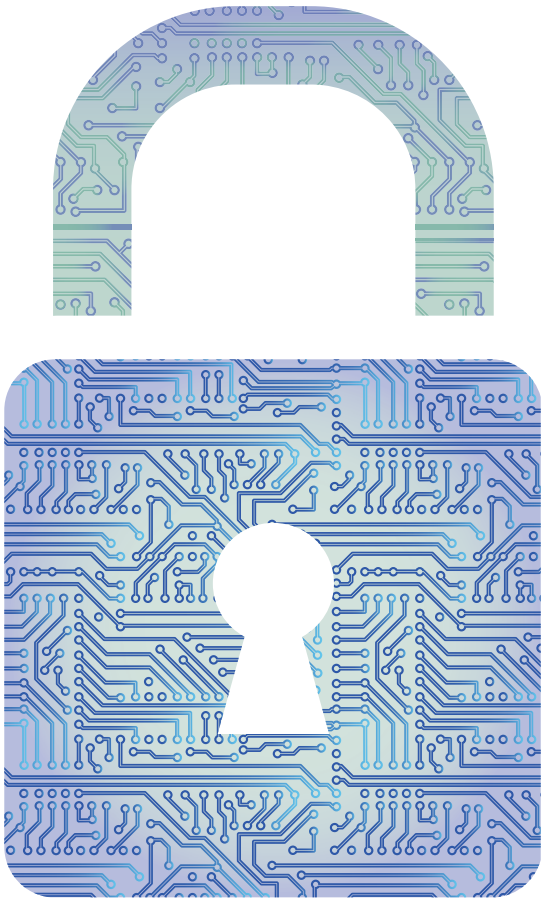


Cyber secure:

Making London business safe against online crime

September 2014

LONDON of CHAMBER
COMMERCE AND INDUSTRY

CONTENTS

London Chamber of Commerce and Industry (LCCI)

LCCI represents London businesses' interests to the Mayor and the GLA, national Government, Parliament and other relevant stakeholders. LCCI's research focuses on business-related matters led by the views and experiences of our member companies and is characterised by its independence and solution-focused approach.

LCCI would like to thank everybody that contributed to this report.

For further information on this report, please contact:

Sean McKee
Director of Policy and Public Affairs
E: smckee@londonchamber.co.uk
T: +44 (0)20 7203 1882

Simon Whalley
Head of External Affairs
E: swhalley@londonchamber.co.uk
T: +44 (0)20 7203 1895

Saif Ullah
Policy Research Officer
E: sullah@londonchamber.co.uk
T: +44 (0)20 7203 1925

FOREWORD

The past year has seen countless media reports of businesses, both big and small, experiencing security breaches as a result of cyber crime. Loss of sensitive data or valuable intellectual property, disruption of services to users, or infected systems from a virus, can all present significant, and sometimes irrevocable, costs to business. As the threat of cyber crime grows and criminals become more sophisticated in their methods, this can present a serious threat to London's reputation as a safe place to do business.

Increasing awareness of cyber threats is central to helping businesses protect themselves from exposure. Firms, particularly small and medium-sized enterprises (SMEs), often have limited resources and are very busy running their day-to-day operations to determine and address their vulnerability to cyber criminals. Quick, easy to adopt, and affordable solutions are likely to be of greater interest to smaller businesses.

Assisting police forces in reducing threat levels is also important. Reporting of online crime remains low and this inhibits authorities' ability to pursue and prevent criminal activities online. Businesses need to be made aware that they can contribute to a safer operating environment by reporting instances of cyber crime, while procedures need to be made clear and simple to reduce the amount of time and effort required from firms to report.

Ensuring that London and the UK is one of the safest places in the world to do business must be a top priority of both the Government and City Hall. London Chamber of Commerce and Industry (LCCI) is supportive of this aim. However, for it to be achieved, government, law enforcement, and business groups have a key role to play by working together to help firms adopt cyber security as a crucial element to their future prosperity.

Finally, I would like to note our thanks to LCCI's Cyber Working Group, part of the LCCI Defence and Security Committee, for informing this report on cyber security.

Colin Stanbridge, Chief Executive, LCCI

1. EXECUTIVE SUMMARY

Ensuring London and the UK is a safe place to do business must be a key priority to both the Government and City Hall. However, businesses and the economy are under serious and growing threats from cyber crime. Cyber attacks are estimated to cost UK companies tens of billions of pounds a year. The real impact of cyber crime is likely to be far greater, with a significant number of cyber attacks going unreported each year. The Government has taken measures to bolster the cyber security landscape but London businesses remain susceptible to basic cyber attacks, and indications are that smaller firms in particular are struggling to grasp the implications of cyber threats to their operations.

The reputation of London as a major global centre for business is particularly vulnerable to the rising threat of cyber crime. Cyber criminals are increasingly targeting SMEs (who account for the vast majority of the capital's private sector enterprises) perhaps because they are perceived as "weak links" in a supply chain. A major cyber attack on London's critical infrastructure, impacting on the transport or energy networks, or financial services, could also cause the capital's economy to grind to a halt.

In order to assess the cyber security challenge faced by London business, this report explores the incidence and impact of cyber crime to London businesses, highlights the barriers firms face in addressing cyber threats, offers solutions to improve protection, and outlines ways in which current systems for response and redress of cyber crime can be modified to reduce the cost to victims.

The following findings and recommendations are based on a survey of members and in-depth interviews, and consultations with London businesses and other stakeholders of all sizes and from all economic sectors.

i) Lack of awareness of cyber threats is one of the main barriers for London businesses in addressing cyber crime

The Government has taken steps to stimulate greater interest in cyber security among businesses, but the large number of departments and agencies involved in the delivery of the National Cyber Security Programme can make it difficult for firms to know where to go for guidance.

Information sharing is another way firms can become better aware of cyber threats. The *Cyber Security Information Sharing Partnership* (CiSP) provides a confidential means to do so, but intelligence is often too technical and beyond the level of understanding of most SMEs.

Phishing, hacking and intellectual property (IP) or data theft are the most common forms of cyber crime affecting London businesses. London's growing technology and digital sector in particular could find itself under greater threat from cyber criminals targeting their valuable IP and confidential data, undermining London's reputation as a safe place to do business.

Recommendation 1: To build upon existing awareness campaigns, the Government should look to create a single 'landing pad' aimed at businesses that signposts all relevant cyber security material. This would make it simpler for businesses to know where to go for cyber security advice.

Recommendation 2: To help SMEs get the most out of the portal, the *Cyber Security Information Sharing Partnership* (CiSP) should be made more easily accessible, and its availability more widely promoted to the business community.

Recommendation 3: The Mayor of London must play a leading role in promoting cyber security resilience among London businesses through the proposed London *Business Crime Resilience Centre*, which can act as a means of raising awareness of cyber security resources, complementing national efforts.

ii) The high cost of protection is the main barrier to London firms' implementation of stronger cyber security measures

Implementing comprehensive cyber security measures can be expensive. Although there are an increasing number of free and low-cost options available to SMEs, such as the Government's *Cyber Essentials* scheme, many companies remain unaware of their availability. Less technical language that is easier to understand would also help to make the available tools more accessible for SMEs.

Many businesses are also unaware of the funding available through the Innovation Voucher for Cyber Security scheme, which itself is subject to uncertain funding cycles and budgetary constraints.

Recommendation 4: To increase take up of the scheme, the Government should look to promote *Cyber Essentials* more widely to SMEs and simplify the language used in the self-assessment documentation in order to make it easier for smaller firms to use. In the long term, *Cyber Essentials* should offer guidance for companies to protect themselves against more advanced online threats.

Recommendation 5: To help more businesses, particularly SMEs, meet the high cost of cyber security, the Government must keep its Innovation Voucher for Cyber Security open on a continuous basis, unconstrained by budgetary considerations, while also better promoting its availability, and demonstrating how it could help firms attain the *Cyber Essentials* badge.

iii) Cyber crime is under-reported to police authorities as London businesses do not view it as a criminal offence

Cyber crime is often viewed by businesses as an issue to be resolved by their IT departments. The reporting process can be seen as a waste of time and potentially detrimental to a business, since it could impact their reputation if a breach became public knowledge. *Action Fraud* provides companies with a single point for reporting cyber crime, but lacks sufficient advertising or an adequate reporting process.

Recommendation 6: To help improve the number of businesses that recognise and report cyber crimes to authorities, *Action Fraud* should offer clear definitions of what constitutes cyber crime, manage business expectation of the actions taken following a report, minimise the amount of information required from businesses, and promote its existence in places such as the single landing pad and the London *Business Crime Resilience Centre*.

iv) The complexity of the UK legal system prevents businesses from seeking redress and compensation from cyber crime

Businesses can seek redress against cyber criminals through both civil and criminal procedures, yet navigating the UK legal system can be difficult and firms may not be aware of the options available to them to seek redress.

Cyber Liability Insurance Cover (CLIC) can help businesses recover costs following a cyber attack, but the UK market for cyber liability insurance remains small and the lack of actuarial data means prices for purchasing cyber insurance can be prohibitively high.

Recommendation 7: The Government should encourage Internet Service Providers (ISPs) and banks to disclose information on the origins of cyber crimes more quickly so that authorities and lawyers can take faster and more decisive action against perpetrators. The Government should also provide simple guidance for SMEs on how they can seek cyber-related redress through the civil or criminal legal system.

Recommendation 8: As well as *Cyber Essentials*, the Government and the Mayor of London should promote the availability of *Cyber Liability Insurance Cover* (CLIC) more widely in order to protect against cyber threats. Increased take up of cyber cover will help lower the cost of premiums to businesses in the long term and provide a means of seeking compensation against cyber crimes.

2. THE GROWING THREAT OF CYBER CRIME

The rapid growth of the internet has transformed the way in which UK companies do business. UK companies are estimated to earn £1 in every £5 through the "internet economy", and the internet-related marketplace alone is estimated to be worth £82 billion.[1] However, as more and more organisations look to capitalise on opportunities available to develop their business within the digital world, their risk of exposure to criminal elements that their organisation may not be ready to counter increases. These criminal activities, commonly referred to as "cyber crime", are largely present only in the digital world and can result in significant financial losses for business.

Businesses are most often a target for cyber criminals because they hold data or personal information that is of significant financial worth within criminal networks. Hackers that obtain data from companies, such as names, email addresses or financial information, can sell this information to a variety of buyers, including identity thieves, organised crime rings or spammers, who can then use the data for personal profit.[2]

Cyber criminals may also target businesses for their valuable intellectual property or trade secrets, significantly harming a firm's competitiveness. Depending on the motivation of the cyber attackers, firms may also be hit with costs through system or website downtime, recovery after an attack, or through less measurable costs such as reputational damage and legal implications.[3] Companies are therefore a lucrative target for cyber criminals, and the impact on the business in terms of cost can be huge.

Measuring the cost of cyber crime to businesses can be difficult as there is no universally recognised definition of "cyber crime".[4] The Government defines cyber crime as:

The illegal activities undertaken by criminals for financial gain, which exploit vulnerabilities in the use of the Internet and other electronic systems to illicitly access or attack information and services used by citizens, business and government.[5]

Cyber crime is estimated to cost the economy £27 billion per year when accounting for its impact on UK consumers, government and businesses. **However, the cost of cyber crime to UK companies alone is estimated to be at least £21 billion per year.**[6]
The real cost of cyber crime could in fact be far higher due to widespread under-reporting to authorities.[7] The average cost of security breaches experienced by smaller and large businesses has also increased significantly in the last year.[8] Companies of all sizes are vulnerable to different types of cyber attack; the type of breach and its overall cost is usually dependent on the motives of the cyber criminals (see Table 1).

[1] AT Kearney (2012): *The Internet Economy in the United Kingdom*
[2] CIO: *Are you at risk? What cyber criminals do with your personal data*, 26 January 2012
[3] Department for Business, Innovation and Skills (BIS) (2014): 2014 *Information Security Breaches Survey*, p.16
[4] Different definitions agree on the significant role of networked technologies to enable this form of criminal activity. But some definitions broaden the criteria to include other illicit activities carried out on the internet. More information can be found on the Swansea University "*Cybercrime and Cyberspace*" page, at http://hocc.swansea.ac.uk/node/100
[5] Detica and Cabinet Office (2011): *The cost of cybercrime*, p.6
[6] Ibid, p.3
[7] Ibid, p.5
[8] The worst security breach for a large organisation cost on average between £600,000 – £1.15 million (up from £450,000 – £850,000 a year ago), while for a small business this amounted to £65,000 - £115,000 (up from £35,000 - £65,000 a year ago). BIS (2014), p.2

Table 1: Examples of cyber threats and attacks

Type of threat[9]	Examples of attacks
Online fraud and criminal activity – exploiting businesses for financial gain, such as stealing confidential data or valuable intellectual property. Phishing emails containing malicious software are a typical entry point in this type of cyber threat.[10] The use of ransomware – malicious software that restricts a computer system and demands payment for it to be removed – is a growing financial threat to businesses.	eBay's database was hacked in mid-2014, which included customer names, email address, physical address, phone numbers and dates of birth. **Up to 145 million customers were affected and share prices fell by more than 8% immediately after the attack.**[11] Computers around the world were infected by a particularly malicious form of ransomware circulated by email in 2013 and 2014. The ransomware rendered machines of individual users and businesses unusable until each **paid a ransom worth hundreds of pounds.**[12]
"Hacktivism" – politically or morally inflected attacks that involve humiliating or vandalising a company's public profile, or making their systems inaccessible to service users.[13]	Internet payment website PayPal was hit by a persistent attack from August 2010 to January 2011 that flooded its system with an enormous number of online requests in order to slow them down and eventually take them offline. The cost was a slowdown of its service to customers, three weeks of repair time from over 100 workers, and the implementation of new software and hardware to defend against similar attacks in the future. **The total cost to the firm was estimated at £3.5 million.**[14]
Industrial espionage – stealing valuable trade secrets or intellectual property to gain competitive advantage. This type of threat is often associated with state-linked groups that target foreign companies in order to boost their own country's industries.	A major London company was estimated to have **incurred revenue losses of £800 million** as a result of a state-sponsored cyber attack. This loss stemmed from intellectual property loss and commercial disadvantage in contractual negotiations.[15]
Cyber warfare – targeting businesses closely linked to national infrastructure, thereby weakening the resilience of the state.	Cyber attacks between Ukraine and Russia have escalated in recent months, ranging from attempts to damage computer systems, steal intelligence, or simply spread online propaganda.[16]

[9] Types of threats listed outlined in Financial Times: *Cyber security: business is in the front line*, 29 April 2014
[10] *Phishing* involves emails disguised as trusted individuals or organisations aimed at tricking targets to click a link or open an attachment that contains malicious software. Once clicked, the malware is downloaded on to the recipient's computer, giving the attacker access to information, such as bank accounts.
[11] The Telegraph: *eBay admits cyber attack has hit sales*, 16 July 2014
[12] For more information, see Get Safe Online: *We have short time to beat a powerful computer attack*, Press Release, 2 June 2014
[13] Attacks that involve systems becoming inaccessible to service users are often referred to as *Distributed Denial-of-Service (DDoS)*.
[14] BBC: *Anonymous hackers 'cost PayPal £3.5m'*, 22 November 2012
[15] Computing: *Corporate espionage on 'an industrial scale' targeting the UK*, 26 June 2012
[16] The Telegraph: *Ukraine cyber war escalates alongside violence*, 28 May 2014

While it is often major information breaches at large corporations that are reported in the media, SMEs are just as, if not more, vulnerable to the same cyber threats. *Phishing* emails are one route of entry for cyber criminals into SMEs, as the example below illustrates.

> *"The phishing emails I received looked genuine and even I, a security specialist, made the classic mistake of opening an attachment, which resulted in ransomware from hackers being installed onto my computer. Fortunately, it was picked up by security software that I had installed on my computer, and the only financial cost I had to pay was to an IT company to ensure the malware was correctly removed. If I didn't have security software installed, the cost would have been far greater".*
>
> Director of a small security firm

Smaller businesses are considered easier targets for cyber criminals because of their less sophisticated security measures.[17] SMEs may also be targeted because cyber criminals see them as an easy entry point into high-value business supply chains.[18] For example, US company Target, which lost 70 million customer details last year after its system was compromised, said that the hackers were able gain access to its data through a contractor.[19]

> *"A lot of large companies are now scrutinising the security measures of businesses in their supply chain in order to prevent cyber criminals from using those firms as a means of entry. SMEs need to start thinking more about their security measures if they hadn't done so in the past".*
>
> Associate Director of a large business consultancy

However, many small and medium-sized businesses do not believe that they are at risk of a cyber attack. A recent global survey found that three-quarters (75%) of SMEs felt their business was too small to be of interest to cyber criminals, while over half (59%) believed that the information that they held would be of no interest to cyber criminals.[20] This is despite the fact that targeted attacks aimed at smaller businesses around the world accounted for 30% of all such attacks, peaking at 53% by the end of the year.[21] SMEs are being increasingly targeted by cyber criminals, and unless they become more aware of cyber threats and do more to protect themselves, they will be more vulnerable to cyber attacks.

> *"If a small business holds some form of important intellectual property or personal data, then it is just as much of an interest to a hacker as any large organisation. In fact, cyber criminals may be more interested in smaller businesses because their systems are easier to break into. Many SMEs won't have the same security products or IT staff to monitor their network, which makes them easier to hack. SMEs need to understand that they are absolutely of interest to hackers".*
>
> Managing Director of an IT security firm

While businesses incur the majority of costs arising from cyber crime, public infrastructure assets are also increasingly under threat. **Cyber attacks on key national infrastructure targets, such as the energy network, telecommunications, financial services, and transport sectors, have the potential to cause major disruption to services on which London firms depend**. The technology running the world's critical infrastructure is increasingly at risk of cyber attack.[22] Plots targeting power and energy companies by international and often state-sponsored groups have been uncovered in recent

[17] Financial Times: *Cyber criminals target smaller companies*, 10 February 2014
[18] Ibid.
[19] The Guardian: *Cyber attack on Pennsylvania company possibly linked to Target data breach*, 7 February 2014
[20] Smaller businesses are defined as between 1-250 employees in the Kaspersky Lab poll, cited in Computer Weekly: *SMEs believe they are immune to cyber attack*, 17 March 2014
[21] Symantec (2014): *Internet Security Threat Report 2014*, p. 30
[22] Computer Weekly: *Cyber threat moving to critical infrastructure, study shows*, 9 April 2014

months[23] and the growing volume of electronic information shared by passenger aircraft to external systems could make flight networks more vulnerable to cyber threats.[24] Cyber security measures at healthcare facilities have recently been placed under the microscope following several notable breaches of patient information.[25]

The Bank of England has sought to improve the resilience of the financial sector to cyber attacks through regular 'cyber drill' exercises, the latest of which, Operation Waking Shark II, took place in mid-November 2013.[26] Business sectors that are critical to the basic functioning of the London economy should be adequately prepared to counter significant and emerging cyber threats. **The combination of the increased incidence of cyber crime against businesses and against the critical infrastructure on which they depend could put London's reputation as a safe place to do business in jeopardy**.

> *"When people think of cyber crime, their thoughts instantly gravitate towards the hacking or stealing of bank records and sensitive information. They probably don't understand the knock on effect of cyber crime against very small businesses. My business experienced two hacking attempts that brought down our servers, essentially closing down my business while my small team of workers tried to rectify the issue. I think that's probably a bigger cost to the economy than stealing bank details. I feel that the Government could be more engaged in helping small businesses understand those costs".*
>
> Director of a creative branding agency

To better understand the impact of cyber crime on London business, LCCI conducted a poll of its members.[27] **The results found that over half (54%) of London businesses had been hit by a cyber attack in the last 12 months**. Attacks that involved phishing, hacking or the eventual theft of confidential data or intellectual property (IP) were the most common form of cyber crime, cited by 44% of London businesses (See Figure 1). This was followed by infection by viruses or malicious software, affecting almost a third (32%) of London companies. System security breaches resulting in denial of service were relatively rare, with only one in twenty London businesses reporting to have been victimised in this way.

While 38% of companies said that they had not been the victim of cyber crime in the last year, our interviews with London businesses suggest that many could be unaware of what officially constitutes a cyber crime. Of the 9% of firms that were hit by another form of cyber crime, examples included online defamation and slowdown in service from internet service providers as a result of attacks on their server.

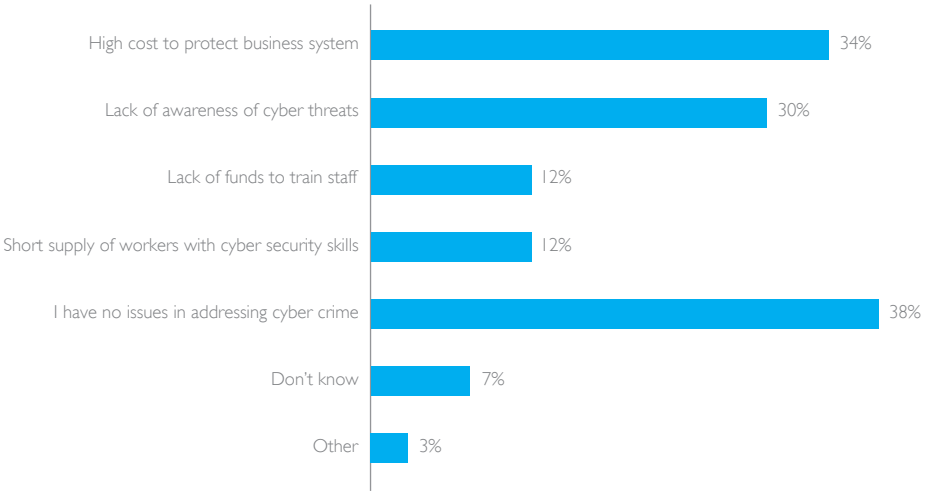
Figure 1: Types of cyber crime affecting London businesses - more than one option could be selected

[23] V3: *Russian 'Energetic Bear' hackers caught ransacking energy companies*, 22 January 2014
[24] The Telegraph: *Cyber terrorism is 'biggest threat to aircraft'*, 27 December 2013
[25] Computing: *Security experts' surprise over report claiming healthcare 'lags behind' in cyber security*, 29 May 2014
[26] For more information, please visit http://www.bankofengland.co.uk/financialstability/fsc/Documents/wakingshark2report.pdf
[27] March 2014 LCCI survey of 127 London businesses

Asked about the main factors preventing them from better addressing cyber attacks, **over a third (34%) of London firms highlighted the high cost of protection as a barrier to implementing stronger cyber security measures** (See Figure 2). Businesses that we spoke to indicated that there was a "perception" among SMEs that implementing strong cyber security measures was expensive and not commensurate to the "risk" that it poses. Some business leaders believed SMEs interpreted the heavy investment by larger organisations into cyber security as meaning that the cost of implementing sufficient cyber security measures for themselves was high.

This perceived low risk versus high cost is preventing companies from allocating resources to cyber security, despite the availability of free and low-cost solutions. A senior consultant at a large business consultancy felt the reason for this was small businesses' poor understanding of cyber crime: *"SMEs don't want to be spending lots of money on cyber security if the risk of cyber crime is quite small, but it's understanding those risks to their business and what they can do to protect themselves that is important. At the moment, this level of understanding among SMEs is quite immature".*

Figure 2: Barriers to addressing cyber threats - more than one option could be selected



This was borne out by our survey, as **30% of London firms felt they lacked awareness of cyber threats** (See Figure 2). Businesses interviewed suggested that SMEs did not really understand the knock-on impact of cyber crime on their operations; it was only once a company was hit by a cyber attack that steps were taken to implement stronger cyber security measures.

Budget constraints to train staff and a short supply of workers with cyber security skills were also each highlighted as barriers to addressing cyber crime by 12% of London businesses.

With low awareness and perceived high cost being the main barriers for business readiness for cyber crime, the following sections examine how these can be addressed. This is followed by an examination of how businesses respond to cyber attacks and an outline of the ways in which they can seek redress and recover costs from online crime. Finally, we assess the overall impact of cyber crime on the capital, highlighting measures by which government, police authorities and business can work together to counter cyber threats and maintain London's standing as a safe place to do business.

3. RAISING AWARENESS

A lack of awareness of cyber threats is preventing 30% of London businesses from effectively guarding against cyber crime. The Government has taken steps to address this and stimulate greater interest in adopting cyber security measures among firms.

In 2011, the Government launched a four-year National Cyber Security Programme, overseen by the Cabinet Office, aimed at countering cyber crime. The programme seeks to promote the UK *"as one of the most secure places in the world to do business in cyberspace"* and to create *"a vibrant, resilient and secure cyberspace"* in the UK by 2015, by helping individuals, businesses and key UK infrastructure improve their resilience to cyber attacks.[28] The Government has allocated £860 million to achieve the programme's goals.[29]

Guidance notes on cyber security have also been published to make it easier for businesses to protect themselves.[30] More recently, the Government launched the *Cyber Streetwise* campaign, which aims to improve SMEs and individuals' awareness and ability to protect themselves against cyber threats.[31] The campaign includes a dedicated website to provide individuals and businesses with clear actions for protection against cyber crime. While the campaign has generated public interest in the *Cyber Streetwise* website and connected YouTube videos,[32] it is too soon to tell whether this has translated into improved cyber security implementation among its target audience.

> *"When we hear about cyber security it always tends to be at the individual level rather than business level. Businesses have a commercial interest in being secure, and in reassuring our clients that their security is not compromised. The Government has to understand that we're the backbone of the economy and while it is commendable that they come up with initiatives like Cyber Streetwise, I think it is more for consumers and the home. They need to reach out more to businesses".*
>
> Communications Director of a medium-sized procurement and export company

Get Safe Online, a joint government-private sector funded initiative formed in 2006, has also played a prominent role in improving education and awareness of cyber security measures to businesses.[33] For example, in recent months *Get Safe Online* has worked closely with the National Crime Agency (NCA) to urge companies to take action against the imminent threat posed by two forms of malicious software, which were circulating worldwide and known to have taken hundreds of millions of pounds from infected computers.[34]

While the Government has made attempts to improve awareness of cyber threats, our survey results indicate that London firms remain unclear about why cyber security is relevant to their business. The myriad government agencies involved in delivering the cyber security programme can make it difficult for businesses to know where to go to access cyber security guidance. *Cyber Streetwise*, *Get Safe Online* and BIS guidelines, Home Office, Cabinet Office, Government Communications Headquarters (GCHQ), the National Crime Agency, law enforcement bodies and others are all involved in the delivery of the programme. **To make it as easy as possible for businesses to access cyber security guidance, the Government should look to develop a single 'landing pad' for companies to access its broad range of cyber security advice**. This single reference point for cyber security should point businesses to other resources should they require more specialist advice. The *Cyber Streetwise* website could

[28] Cabinet Office (2011): *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world*, p.8

[29] The National Cyber Security Programme was initially allocated £650 million, but following the 2013 Spending Review, a further £210 million was allocated to the programme until 2015.

[30] BIS has published guidance notes on *10 steps to cyber security*, and *Small businesses: what you need to know about cyber security.*

[31] For more information about *Cyber Streetwise*, please visit https://www.cyberstreetwise.com/

[32] *Cyber Streetwise* promotional videos have generated over 1 million hits on YouTube since published on 23 December 2013. See https://www.youtube.com/playlist?list=PLsQNBGK6c5kHXt7_rkVk4HGVVI006t3AI

[33] For more information about *Get Safe Online*, please visit https://www.getsafeonline.org/

[34] In early June 2014, *Get Safe Online* and the National Crime Agency (NCA) issued a joint press statement for the public and small businesses to take action to protect themselves against the *Gameover Zeus* and *CryptoLocker* viruses. For more information, see Get Safe Online: *We have short time to beat powerful computer attack*, Press Release, 2 June 2014

potentially fulfil this role of a single landing pad. Such a portal would be particularly helpful for SMEs, who are less likely to have the time or resources to determine what cyber security measures are relevant to them. Firms could be informed of the landing pad at key stages of their life cycle, for instance when registering at Companies' House, opening a business bank account, or applying for a loan. The Government should work with industry partners to ensure information is distributed in a targeted manner.

Recommendation 1: To build upon existing awareness campaigns, the Government should look to create a single 'landing pad' aimed at businesses that signposts all relevant cyber security material. This would make it simpler for businesses to know where to go for cyber security advice.

Firms can become better aware of cyber threats by sharing more information with one another. In order to promote this, the Government launched the *Cyber Security Information Sharing Partnership* (CiSP) in March 2013, an online portal that allows firms to confidentially share details of online attacks and threats experienced with other users.[35] *CiSP* is open to all businesses and is free to join.[36] Management of *CiSP* is overseen by the *UK National Computer Emergency Response Team* (CERT-UK), which acts as a central point for coordination and enhancement of UK cyber resilience, and provides intelligence to Government and *CiSP* members on new and emerging threats.[37]

LCCI welcomes the creation of *CiSP* to support business awareness of cyber threats. So far, however, *CiSP* has struggled to attract many businesses to join its sharing facility. As few as 320 organisations are signed up to *CiSP* at present.[38] **It is also insufficiently clear who *CiSP's* target audience is**. In addition to sharing between members, *CiSP* members receive a weekly Situational Awareness report which provides a summary of threats discussed within the portal. However, much of the intelligence outlined in these reports tends to be of more advanced attacks, which are less relevant and often beyond the level of understanding of most SMEs.[39] ***CiSP*, as an information sharing portal, is not sufficiently accessible and is too difficult to navigate for the majority of SMEs**.

As a mechanism for sharing threat advice, *CiSP*, in its current format, does not meet the needs of the majority of London firms looking to gain a better understanding of cyber threats. To ensure that *CiSP* is fit for purpose, the Government should be clear about who it sees as the main audience for the portal. If the Government sees *CiSP* as an important mechanism for SMEs to gain advice on cyber threats, then businesses need to be made more aware of the portal's existence, and information provided on the site needs to be made as clear and as simple to understand as possible in order to appeal to less technical users.

Recommendation 2: To help SMEs get the most out of the portal, the *Cyber Security Information Sharing Partnership* (CiSP) should be made more easily accessible, and its availability more widely promoted to the business community.

As our survey results indicate, phishing, hacking and the eventual theft of intellectual property (IP) or data is the most common form of cyber crime affecting London firms (44% had been hit by this form of attack in the last 12 months). IP theft is already estimated to cost UK businesses £9.2 billion per year,[40] making it the most costly form of cyber crime. However, with IP-dependent companies making an increasingly important contribution to the capital's economy, London's burgeoning technology and digital sector in particular could find itself under greater threat from cyber criminals targeting their valuable IP and confidential data.[41] This has the potential to undermine London's reputation as a safe place to do business.

[35] For more information on *CiSP*, please visit https://www.cisp.org.uk/
[36] All individual applications are assessed prior to access being granted.
[37] For more information on *CERT-UK*, please visit https://www.cert.gov.uk/
[38] CERT-UK (March 2014): *Fusion CiSP Non-Member Edition*
[39] Extracts of the CiSP Situational Awareness Weekly Report can be found at https://www.cert.gov.uk/resources/news/
[40] Detica and Cabinet Office (2011), p.2
[41] Since Tech City was founded in East London in 2010, the number of technology and digital firms in London has increased by 76%, boosting employment numbers. Tech City (2013): *Tech City Annual Report 2013*

Indeed, IP-dependent firms, such as those in the technology and digital sector, are considered most at risk of cyber attacks[42] but indications are that **businesses of all sizes and sectors are experiencing a greater volume of IP breaches**. Cyber attacks designed to steal commercial secrets doubled in the year 2012-13 compared to the previous financial year and attacks on small businesses have increased significantly (by 50% year on year).[43]

The Mayor of London is taking steps to support London businesses in tackling this growing area of cyber crime. The Mayor's Office for Policing and Crime (MOPAC) published its *Business Crime Strategy* in July 2014, a three-year programme aimed at improving the landscape for businesses to protect their physical assets and intellectual property.[44]
The strategy includes plans to create a London *Business Crime Resilience Centre*, a hub designed to promote collaboration between London companies, the police and the public sector through information sharing on criminal threats to firms, such as cyber crime. A similar model has been operating in Scotland.[45]

> *"Educating employees is key to improving cyber security in small businesses. Cyber criminals are after things that are unique and have value in the outside world, and it costs nothing for them to catch businesses out through spam and phishing emails. The best way to promote cyber security to small business owners is to provide them with concrete examples of what is actually valuable, such as their price list. It is a lack of awareness of what cyber criminals are after that can lose you things of value. This is not yet being put into context".*
>
> Chief Marketing Officer of an information security company

MOPAC has a greater role to play than it has done so far in protecting London firms from IP theft and data breaches. The proposed London *Business Crime Resilience Centre* should concentrate on getting London businesses more engaged in cyber security preparation by making them aware of resources already available, such as *CiSP*, *Cyber Streetwise*, *Get Safe Online* and government guidance notes, and disseminating existing guidance to firms in need of support. A regional focal point would provide the higher level of engagement required by London firms to understand why implementation of cyber security measures are a growing necessity, without undermining the work of national authorities.

Recommendation 3: The Mayor of London must play a leading role in promoting cyber security resilience among London businesses through the proposed London *Business Crime Resilience Centre*, which can act as a means of raising awareness of cyber security resources, complementing national efforts.

[42] Firms such as software, financial services, pharmaceuticals and electronics are particularly at risk of IP theft. Detica and Cabinet Office (2011)
[43] Statistics quoted from Kroll and Symantec in Financial Times: *Symantec chief warns over cyber threat to intellectual property*, 25 November 2013
[44] Mayor of London Office for Policing and Crime (2014): *Business Crime Strategy 2014-16*
[45] For more information on the *Scottish Business Resilience Centre*, please visit http://www.sbrcentre.co.uk/pages/1752/1/Cyber_and_eCrime.html

4. COST OF CYBER SECURITY

Small companies often operate on tight resources, lacking time, money or manpower to dedicate to activities not seen as crucial to the running of their business. Many SMEs do not feel they have the time or resources available to better protect themselves against potential cyber attacks. This is illustrated in our survey results, which indicate that over a third (34%) of London firms see the cost of cyber security as prohibitively high (See Figure 2).

Implementing comprehensive cyber security measures can be costly. *ISO 27001*[46] – a recognised international standard in information security – helps businesses employ a robust cyber security structure and earn accreditation. Implementation of its Information Security Management System (ISMS) goes beyond standard security practices, such as installing up to date anti-virus software and firewalls, instead imbedding a culture of information security across the organisation through its employees, processes and IT systems.[47] While the total cost of implementation tends to depend on the size of the organisation, the overall cost tends to be prohibitively expensive for smaller businesses.[48]

However, there are an increasing number of free and low-cost cyber security options available to businesses. Several high-street banks offer free security software if you use their online services, while *Get Safe Online* provides information on several free security tools made available by internet security companies.[49] As a low-cost alternative to the *ISO 27001* international standard, the IASME Consortium has created the *IASME standard*, which is designed to be more affordable and achievable for small businesses.[50] The process for attaining the *IASME standard* involves continuous assessment, with first certification obtained after the first cycle, followed by intermediate assessments annually and a re-assessment after three years.[51]

In June 2014, the Government launched its *Cyber Essentials* scheme, designed to help businesses develop basic cyber security solutions at an affordable cost.[52] *Cyber Essentials* focuses on key measures that can be implemented by companies to withstand cyber attacks, such as setting up of firewalls, up-to-date malware protection, patch management and appropriate access control to systems.

Two levels of certification can be attained by SMEs under the scheme: the more basic and low-cost *Cyber Essentials*, which requires businesses to self-assess their implementation of specified cyber security measures via a questionnaire signed-off at board management or equivalent business-owner level and verified by an independent certification body; and the more advanced and costly *Cyber Essentials Plus*, which involves independent assessment of an organisation's cyber security approach.[53] Basic *Cyber Essentials* certification can be purchased for £300.[54] The Government has specified that from 1 October 2014, all suppliers bidding for some public sector contracts will need to be certified against the *Cyber Essentials* scheme.

Cyber Essentials is a welcome step forward in getting more small businesses to implement basic and recognised cyber security protection at a low cost. However, for the scheme to gain traction among the business community, companies need to be made more aware of its availability, and provided clearer information on which government contracts it applies to and when these will require them to be certified against *Cyber Essentials*. The language used in self-assessment questions is also too technical for many SMEs to understand.

[46] For more information on *ISO 27001*, please visit http://www.itgovernance.co.uk/iso27001.aspx#.U7VVF7HpAZc
[47] Ibid.
[48] Total cost of implementing *ISO 27001* would include: initial risk assessment to determine level of protection needed; cost of literature and training of employees; cost of external assistance (consultant); cost of technology; cost of employees' time; and cost of certification. More information can be found at http://blog.iso27001standard.com/2011/02/08/how-much-does-iso-27001 implementation-cost/
[49] For more information on *Get Safe Online*, please visit https://www.getsafeonline.org/
[50] For more information on the *IASME standard*, please visit http://www.iasme.co.uk/index.php/standard#
[51] The IASME Consortium: *The Standard for Information Assurance for Small and Medium Sized Enterprises* (IASME) Issue 2.3-2013
[52] For more information on *Cyber Essentials*, please visit https://www.gov.uk/government/publications/cyber-essentials-scheme-overview
[53] HM Government (2014): *Cyber Essentials Scheme: Summary*, p.6
[54] IASME Consortium: *Cyber Essentials Scheme*, at https://www.iasme.co.uk/index.php/cyberessentialsprofile

"Smaller businesses may receive a spear-phishing email from someone that they know, yet once they open it and click on the attachment, they're already downloading malicious software that could be used to take data from their network. Training people to be suspicious is the best thing, so that they think before they click on something".

Managing Director of an IT security firm

For some small firms, basic cyber security measures will help protect them from low-level threats. However, **_Cyber Essentials_ will do little to protect businesses from more advanced online threats**. Highly targeted attacks[55] are being increasingly used by cyber criminals against firms[56] and can be extremely difficult to spot. If employees within an organisation are insufficiently wary of these potential online threats, then there is little that basic firewall and security software can do to prevent a cyber criminal from penetrating a business' system. As *Cyber Essentials* only measures a firm's level of protection at a given point in time, it does not provide the ongoing assessment required to change the culture of a business. Beyond the welcome foundation that *Cyber Essentials* provides, as the scheme evolves it should look to provide a clear path beyond *Cyber Essentials Plus* to offer more advanced protection to businesses.

Recommendation 4: To increase take up of the scheme, the Government should look to promote *Cyber Essentials* more widely to SMEs and simplify the language used in the self-assessment documentation in order to make it easier for smaller firms to use. In the long term, *Cyber Essentials* should offer guidance for companies to protect themselves against more advanced online threats.

Businesses that find the cost of implementing cyber security measures a barrier to improving protection can apply for funding through the Government's Innovation Voucher for Cyber Security scheme. Managed by the Technology Strategy Board, the Innovation Voucher is worth up to £5,000 and is open to SMEs, entrepreneurs and early stage start-ups that want to secure their ideas and business. Eligible companies can use the voucher to secure specialist consulting and services to: help protect their new inventions and business processes; 'cyber audit' their existing processes; move online and develop a technology strategy; develop an idea into a working prototype; and build cyber security into the business from the very beginning.[57]

Innovation Vouchers for Cyber Security are open for application on three month periods on a continuous basis until the overall funding pot is empty. It is currently open for application until the end of October 2014, but there is no indication that it will re-open if all funding has been allocated. **The Government should ensure that there is a continuous pot of money available to businesses to help meet cyber security costs**.

"We're a small business and when we're trying to learn about how to deliver cyber security, it involves a lot of reading and learning. If we were able to access specialists to do an audit of our security measures and speak to us about potential improvements, it would be a huge help".

Director of a small creative branding agency

The Government must also promote the availability of the Innovation Voucher to businesses more widely. Our survey results indicate that London firms see the cost of cyber security as prohibitively high. Having better awareness of funding that can help them

[55] Highly targeted attacks such as "spear-phishing" are more advanced than phishing emails as they refer to their potential victims with more specific and personal details, in order to increase the likelihood of them opening a malicious attachment or link.
[56] Spear-phishing campaigns rose by 91% in 2013 compared to the previous year. Symantec Corporation (2014): *Internet Security Threat Report 2014*, p. 5
[57] For more information on *Innovation Vouchers for Cyber Security*, please visit https://vouchers.innovateuk.org/cyber-security

meet these costs would increase the likelihood of smaller companies utilising the voucher and improve their protection against cyber threats. Businesses that we spoke to were also largely unaware of the existence of the Innovation Voucher.

The Innovation Voucher should also be more explicitly linked to meeting the cost and attaining the *Cyber Essentials* badge. Companies are able to use the voucher to pay for services and accreditation for the *Cyber Essentials* scheme, although they would not be able to pay for security products. However, current guidance for applicants does not make it clear how businesses can use the voucher to obtain *Cyber Essentials*. Connecting the two schemes would incentivise more London firms to pursue *Cyber Essentials* certification if they are able to cover its cost, and thereby improve their level of online security while providing visible evidence of their cyber security proficiency to others.

Recommendation 5: To help more businesses, particularly SMEs, meet the high cost of cyber security, the Government must keep its Innovation Voucher for Cyber Security open on a continuous basis, unconstrained by budgetary considerations, while also better promoting its availability, and demonstrating how it could help firms attain the *Cyber Essentials* badge.

5. RESPONSE

As well as being aware of cyber threats and solutions relevant to their business, it is important for firms to know what to do and where to go in the event of a cyber attack. When London businesses were asked if they knew where to go if hit by a cyber attack, while 65% said they knew what their first port of call would be, **nearly half (48%) cited their IT specialist or IT department**. The result implies that cyber attacks are not being seen as a crime, but rather an IT issue.

Part of the explanation for this may be due to businesses not being clear about the parameters that define a cyber crime. Indeed, LCCI survey results showed that **38% of London firms did not think they had been a victim of cyber crime in the last 12 months**. Yet, many victims are unaware that they had been a victim of a cyber crime as highlighted by a recent survey, which showed that 82% of small companies in the UK believe they are not a potential target for hackers and cyber criminals.[58] **This results in a gap in reported cyber attacks to police authorities**.

Simple examples and case studies of what constitutes a cyber crime would help businesses understand when they have been a victim of cyber crime and when they should be reporting. Easy to understand descriptions of the cyber crimes that firms should be reporting would help them to recognise what to do in such instances.

Businesses may also lack awareness about where to go and what to do in the event of a cyber attack. The Government has tried to make it easier for firms to report cyber crime to authorities. In 2013, *Action Fraud* was established for individuals and companies to report fraud and internet crime.[59] However, *Action Fraud* was not originally set up to have the capability to deal with all reports of cyber crime across the country and was stretched in its capacity to respond to cases. All crime cases and information reported to *Action Fraud* are now passed on to the City of London Police's *National Fraud Intelligence Bureau*, who analyse the reports to build intelligence on cyber threats.[60] The UK's capacity to investigate and pursue cyber criminals on a national and international level has also been enhanced by the creation of the *National Cyber Crime Unit* in spring 2013.[61]

However, many London firms may not be aware of *Action Fraud*. *Action Fraud* must do more to promote its role as the reporting centre for cyber crime, including places such as the single cyber security landing pad and MOPAC's proposed London *Business Crime Resilience Centre*, so businesses are more aware of where they should report a cyber crime.

Business leaders must also take more responsibility for protection and reporting cyber crime, rather than deferring incidents to their IT teams. Businesses should have clear lines of responsibility for reporting cyber crime to authorities. However, IT professionals should also be equipped with the knowledge and skills they need to effectively respond to cyber crime, so that they can provide advice to senior management when incidents are referred to them. Institutions that support the development of IT professionals, such as *BCS - the Chartered Institute for IT* could help IT staff develop this knowledge and support businesses with their overall response to cyber attacks by including cyber crime resilience and criminal response procedures in their professional course syllabi.

Although the number of cyber crimes reported to police increased significantly in 2014,[62] **under-reporting of cyber attacks is well established**. A Government study of

[58] Computing: *Small businesses convinced they won't be cyber attack targets have 'heads in the sand'*, 18 July 2014

[59] For more information on *Action Fraud*, please visit http://www.actionfraud.police.uk/

[60] For more information on *National Fraud Intelligence Bureau*, please visit http://www.cityoflondon.police.uk/advice-and-support/fraud and-economic-crime/nfib/Pages/default.aspx#

[61] *National Cyber Crime Unit* brings together specialists from the Police Central e-Crime Unit in the Metropolitan Police Service and SOCA Cyber to investigate and pursue cyber criminals. More information can be found at http://www.nationalcrimeagency.gov.uk about-us/what-we-do/national-cyber-crime-unit

[62] 22,315 cyber crimes were reported to police in the 2013/14 financial year, nearly double the amount recorded the previous financial year. Evening Standard: *Seven out of 10 frauds are now cyber crimes, police chief warns*, 28 April 2014

reporting behaviours by businesses across four sectors found that just 2% of online crime incidents were reported to the police.[63] Compounded by a large rise in adverse media coverage of security breaches in the last year,[64] **fear of causing reputational damage and a feeling that reporting was a waste of time are strong factors in businesses under-reporting of cyber crime**. Having lost several days of business due to a cyber attack bringing down their server, the Director of a creative branding agency was reluctant to lose any more time by reporting to authorities: *"I'm not sure how long it would have taken and there probably would have been no real outcome for us. We were loath to lose any further time doing any administrative reporting"*.

However, **reporting cyber crime to the police provides authorities with intelligence they need to disrupt criminal networks and better protect businesses from cyber threats**. Previously, reports made to *Action Fraud* often resulted in many individuals and companies receiving little or no feedback about the status of their investigation. Its capability to deal with the growing threat of cyber crime has now been bolstered.[65]

> *"It's important for businesses to report cyber crimes, even if they are relatively low cost. If SMEs are all the victim of the same crime, it helps police build intelligence and take coordinated and targeted action against the cyber criminals. Police capabilities of fighting cyber threats originating abroad have improved massively in the last two years and we have a relationship with the National Cyber Crime Unit, Europol, Homeland Security and other law enforcement agencies to pursue and disrupt international cyber criminals".*
>
> Peter O'Doherty, Action Fraud and National Fraud Intelligence Bureau

Action Fraud provides a mechanism for businesses to report cyber crime but it is too difficult a process for many SMEs to complete. In order to simplify the reporting process, *Action Fraud* should minimise the amount of information required from firms when reporting a cyber crime to the core essentials and make this clear from the outset, so that firms do not see it as an arduous process and are not concerned about handing over too much information. At the same time, it should be made clear to businesses that, while reporting to them may not result in specific action taken against perpetrators of their cyber crime, the intelligence gathered can help police reduce the threat, and ultimately reduce cost to business and vulnerability to cyber crime.

Recommendation 6: To help improve the number of businesses that recognise and report cyber crimes to authorities, *Action Fraud* should offer clear definitions of what constitutes cyber crime, manage business expectation of the actions taken following a report, minimise the amount of information required from businesses, and promote its existence in places such as the single landing pad and the London *Business Crime Resilience Centre*.

[63] The four business sectors covered were accommodation and food; wholesale and retail; manufacturing; and transportation and storage. Home Office (2013): *Cyber crime: A review of the evidence*, p.6

[64] Estimated cost caused by reputational damage was £1,600 - £8,000 for small businesses and £50,000 - £180,000 for large organisations. BIS (2014), p. 18

[65] Evening Standard: *Seven out of 10 frauds are now cyber crimes, police chief warns*, 28 April 2014

6. REDRESS AND RECOVERY

Businesses that wish to recover the cost of a cyber crime can use the UK legal system to pursue compensation. The UK legal system is well designed to seek redress through both civil and criminal means. Civil remedies, such as actions for damages, court orders against Internet Service Providers (ISPs) to reveal where a cyber crime originated, injunctions, third party disclosure orders, and breach of confidence, are available to companies in pursuit of compensation.[66]

Court orders against ISPs and banks to disclose intelligence critical to the detection and identification of those behind cyber crime can be an expensive and a protracted process for authorities and lawyers representing victims. **The Government should do more to encourage ISP's and Banks to take full advantage of the protection that the existing legal framework provides them in releasing this intelligence without the need for police production and civil court orders** so that faster and more decisive action can be taken against criminals.

Criminal prosecutions can be sought under the Computer Misuse Act 1990; recent updates to the Act have raised the punishment handed out to hackers that carry out industrial espionage on UK businesses, which can help act as a deterrent to potential perpetrators.[67]

However, **companies may not be aware of the paths they can take to seek redress against cyber criminals**. To make it as easy as possible for businesses to pursue cyber criminals, the Government should provide simple and clear guidance to SMEs on ways they can seek redress both through the civil and criminal legal system. This could be included on the single landing pad and would help smaller businesses identify the legal instruments available to them, given that the majority would not have the resources available to determine paths for redress.

> **Recommendation 7:** The Government should encourage Internet Service Providers (ISPs) and banks to disclose information on the origins of cyber crimes more quickly so that authorities and lawyers can take faster and more decisive action against perpetrators. The Government should also provide simple guidance for SMEs on how they can seek cyber-related redress through the civil or criminal legal system.

While the UK legal system provides options for businesses to pursue damages against cyber criminals, it is difficult to seek redress against attacks that originate from outside the UK. For such instances, or to generally protect your business from losses as a result of cyber crime, companies may want to consider purchasing *Cyber Liability Insurance Cover* (CLIC).

Indeed, the global market for cyber liability insurance has increased significantly in recent years as more companies look to protect themselves from hackers stealing confidential data or shutting down their website. Gross written premiums are expected to total well above $2 billion in 2014, up from an estimated $850 million in 2012.[68] The US makes up the vast majority of this market, where most states have mandatory data breach notification laws.[69]

In comparison, the UK market for cyber liability insurance remains small. The European market for cyber insurance is estimated to be worth $150 million, a fraction of the global market, but it is growing rapidly.[70] Major insurance companies offer cyber liability insurance cover to businesses, while SMEs with IASME accreditation can receive a significant discount on cyber liability insurance through the consortium's partnered provider.[71]

[66] Kennedys: *Cybercrime: risks, penalties and prevention*

[67] The law would have a maximum sentence of 14 years for attacks that create "a significant risk of severe economic or environmental damage or social disruption". See The Guardian: *Life sentences for serious cyberattacks are proposed in Queen's speech*, 4 June 2014

[68] The Telegraph: *Threat from hackers brings rush for extra insurance*, 6 July 2014

[69] 46 out of 50 US states have mandatory requirements for data breach notification. Costs for notifying affected customers can be very high, so mandatory data breach legislation has in part driven the market for cyber security insurance. Computer Weekly: *An introduction to cyber liability insurance cover*, July 2013

[70] Reuters: *Insurers struggle to get grip on burgeoning cyber risk market*, 14 July 2014

[71] For more information, please visit Sutcliffe & Co Insurance Brokers, at http://www.sutcliffeinsurance.co.uk/cyber_liability.aspx

However, because of a lack of actuarial data, insurance companies face difficulties pricing the risk of cyber liability cover by traditional insurance methods. This can mean that prices for purchasing cyber insurance are prohibitively high for SMEs.[72]

New EU Data Protection Regulation could increase the market for cyber insurance in Europe. Proposed changes to EU Data Protection Regulation will require businesses to disclose any data breaches "*without undue delay*".[73] Companies in breach of the Regulation could face a fine of €100,000 or up to 5% of annual worldwide turnover, depending on which is greater.[74] While it may take several years for the Regulation to come into force, it is likely that its eventual implementation will act as a catalyst for growth of the cyber insurance market in Europe, in a similar manner to the expansion of cyber insurance in the US.

The Government's introduction of *Cyber Essentials* certification has been welcomed by the insurance industry as it helps them assess the risk of companies seeking protection.[75] To further assist London businesses in pursuing compensation against cyber crime, the Government and the Mayor of London should look to promote CLIC options available. This would enable firms to protect their losses, particularly from overseas perpetrators. As the cyber insurance market naturally matures, the cost of premiums will decline, making cover more affordable for SMEs. In the long term, a path to more advanced protection through *Cyber Essentials* would enable insurance companies to have greater confidence in accredited businesses' protection from cyber crime. In the meantime, if more insurance companies offer CLIC, and provide a lower-cost offering to firms that are *Cyber Essentials* certified or equivalent, this would support growth in the market and help companies recover damages incurred from cyber crime.

Recommendation 8: As well as *Cyber Essentials*, the Government and the Mayor of London should promote the availability of *Cyber Liability Insurance Cover* (CLIC) more widely in order to protect against cyber threats. Increased take up of cyber cover will help lower the cost of premiums to businesses in the long term and provide a means of seeking compensation against cyber crimes.

[72] Reuters, op. cit.
[73] European Commission: *Data Protection reform makes headway*, October 2013
[74] Ibid, p.5
[75] Hogan Lovells: *UK: Cyber Essentials – Insurance industry backs new government cyber security initiative*, 11 July 2014

7. CONCLUSION

Cyber crime is having a significant impact on London businesses, but measures taken by companies to protect themselves are not commensurate to the risks it poses. With this report, LCCI aims to highlight the reasons why companies are struggling to grasp the necessity of cyber security to their operations, and suggest ways the Government can better support SMEs counter the growing cyber threat. Our research shows that a lack of awareness of cyber threats and a perceived high cost to implementing cyber security were the main factors hindering businesses from improving their online protection measures.

The Government has invested in a National Cyber Security Programme and much of what has been achieved so far has been positive. However, there are clear gaps evident in government's engagement with businesses on cyber security, illustrated by this report's findings.

Educating and making companies aware of why cyber security is relevant to their day to day operations is key to them improving their online protection measures. Smaller businesses do not feel that they are being targeted, placing cyber crime lower on their risk register, yet hackers are increasingly targeting SMEs as an easy way to make a profit or to gain entry into larger businesses whose defences are harder to penetrate. This message is not being taken on board by SMEs. The Mayor of London can help amplify the warnings signalled by the Government to London firms to reach those companies that require more considered engagement.

Awareness of cyber threats is closely aligned to the perceived high cost of cyber security, which businesses seemed to suggest was preventing them from being more cyber secure. Low cost measures are available and can prevent a large number of cyber threats. *Cyber Essentials* is a welcome and affordable means for smaller companies to attain accreditation and standardise protection among SMEs against lower-tier cyber threats. However, more needs to be done to promote its existence and affordability to SMEs.

Police forces require intelligence on cyber crimes to disrupt criminal networks and reduce the overall threat to business. To do this, businesses need to report any cyber attacks that they experience so authorities can build an intelligence picture on current and emerging threats. *Action Fraud* should be more widely promoted so companies are aware of its existence as a central reporting platform, at the same time reassuring firms that their reports will be treated anonymously. Making it easier to navigate the legislative landscape for redress and providing greater and more affordable options for insurance cover will enable businesses to recover faster from major disruptions arising from cyber attacks.

London is a world-leading centre for business, but to maintain its place at the top of the ladder, it will also need to be the safest place to do business. Cyber crime threatens London's standing as a secure place to do business. This must not be allowed to happen if the capital is to remain internationally competitive. To protect the UK's standing, government must continue to dedicate resources towards awareness-raising initiatives and reduce barriers to protection, so that businesses can become *cyber secure*.

ACKNOWLEDGMENTS

LCCI would like to acknowledge the following stakeholders for their assistance during the production of this report:

British Business Federation Authority

CERT-UK

City of London Police

Department for Business, Innovation and Skills (BIS)

Fraud Advisory Panel

Get Safe Online

Home Office

Government Communications Headquarters (GCHQ)

The Mayor's Office for Police and Crime (MOPAC)

Metropolitan Police Service

National Crime Agency

In addition, LCCI would like to thank the members of the LCCI Cyber Working Group for their contribution:

Paul Weatherly, Managing Director, Lockheed Martin UK IS&GS Security (Chair)

Jane Attwood, Security Advisor

Ceri Davies, Security Manager, Interxion

Tarquin Folliss, Director International, Falanx Group

Graeme McGowan, Associate Director, Optimal Risk

Gary Miller, Partner, Mishcon de Reya

London Chamber of Commerce and Industry
33 Queen Street, London EC4R 1AP

T: +44 (0)20 7248 4444
F: +44 (0)20 7203 0391
E: research@londonchamber.co.uk
W: londonchamber.co.uk/research