CYBER RESILIENCE: HOW TO PROTECT SMALL FIRMS IN THE DIGITAL ECONOMY

Published: June 2016

@fsb_policy

fsb.org.uk

fsb

Experts in Business

ACKNOWLEDGMENTS

This paper would not have been possible without the contribution (direct and indirect) of a number of people who have:

- Taken part in numerous discussions about cyber resilience policy and practice over the last 18 months with FSB.
- Provided invaluable insights, comment and critique on earlier drafts of the paper.

There are too many to thank individually. But particular thanks go to FSB members, (especially the Home Affairs Committee) and staff who have contributed so much to the development of this policy paper. Thanks also go to those policymakers, policing and cyber security experts who participated on the panel at FSB's workshop in September 2015 at the Cambridge International Symposium on Economic Crime. Additional thanks go to officials at the Department of Culture, Media and Sport (DCMS), Home Office, the Department of Business, Innovation and Skills (BIS) and HM Inspectorate of Constabulary. Thank you for your knowledge and feedback to both FSB's wider work on cyber resilience and the development of this paper.

Gratitude also go to Giles Herdale, head of digital intelligence & investigation strategy, Professor Ross Anderson, David Porter, Doug Turner (Director, Group Engineering Services at BT) and the Business Emergency Resilience Group. Thank you for sharing your experiences and thoughts on cyber resilience issues.

Finally, FSB would like to acknowledge the ongoing relationship with Cyber Streetwise and their continuing dialogue with FSB about cyber resilience issues. It has proved an invaluable source of insight and assistance.

CYBER RESILIENCE:

HOW TO PROTECT SMALL FIRMS IN THE DIGITAL ECONOMY

66%

of small businesses have been a victim of cyber crime

On average a small business is a victim of

4 cyber crimes

every 2 years

Cyber crime costs each small business victim nearly

£3,000

93%

of smaller firms have cyber crime security measures in place

Types of cyber crime smaller businesses are a victim of

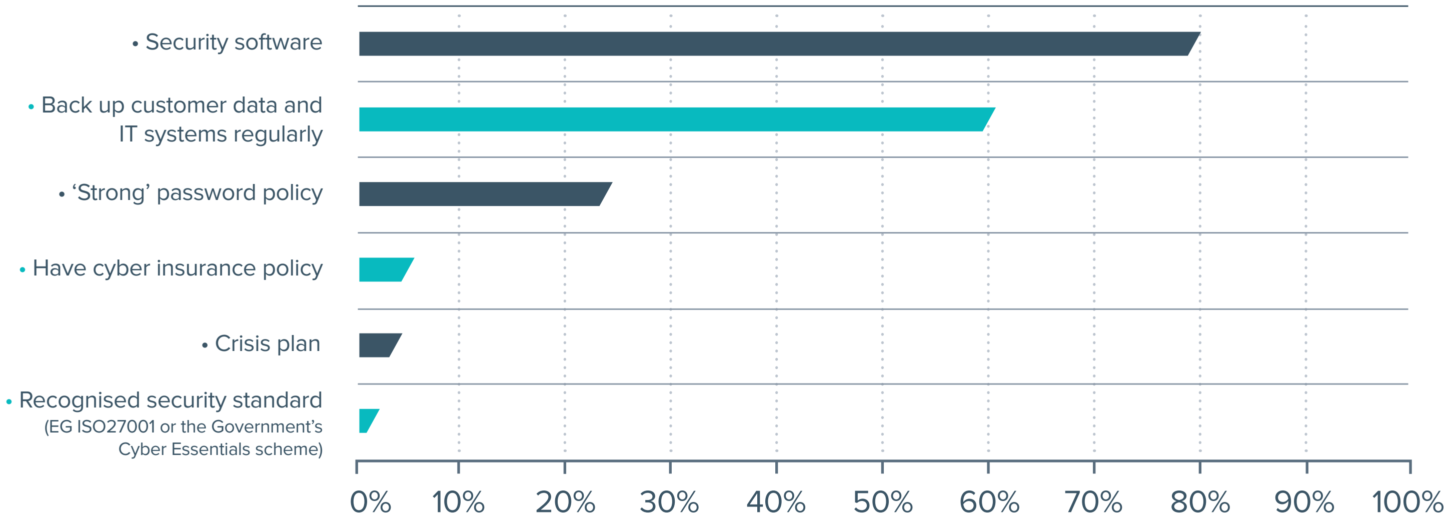
49% - Phishing

37% - Spear Phishing

29% - Malware attacks

10% - Card not present fraud

Security measures against cyber crime in place



All statistics are based on a two year period, ie 2014 and 2015.

CONTENTS

FOREWORD

Over the last couple of decades the economy has shifted towards one that relies on a complex digital communications infrastructure. This offers tremendous opportunities for smaller businesses. The digital economy information age began with personal computing, mobile telephony, the internet and email. It's now moved even further with cloud computing, smart devices – such as tablets and smart phones – and social media. These innovations have helped businesses to reduce costs, increase their efficiency and widen their market reach. The nascent internet of things is going to generate even further opportunities.

However, these benefits have brought with them a wide range of risks for smaller businesses. But not only small businesses. There are equally significant risks for the whole digital communications infrastructure. In a highly interconnected economy a risk for one is a risk for all. The biggest risk comes from the threat of cyber criminality. The latter is a rapidly evolving threat and is in danger of becoming ubiquitous in the digital world.

Recent research by FSB – highlighted in this report – found disturbingly high levels of cyber crime against smaller businesses. Action is needed to improve the cyber resilience of small businesses and the wider economy through:

- Improving the protection levels of the small business community, commercial supply-chains and the digital information networks on which the economy relies.
- Better enabling those impacted by a cyber attack to withstand its effects and prosper again afterwards.
- Improving the law enforcement response to cyber criminality in the longer term.

Successive Governments, from a standing start less than a decade ago have made considerable progress in increasing the cyber resilience of the UK. However, there is more that can and should be done. The key change that needs to take place is a greater sharing of the burden of cyber resilience across business (large – especially those providing the technological and economic infrastructure – and small), Government and individuals. Currently, the burden is not borne by those best able to bear it. Those with the most resources (financial, labour and time) and knowledge at their disposal, are best placed to take the most effective action to reduce the cyber risks, which small businesses and the economy face.

This report looks at the scale and scope of cyber crime against small business and how the burden of resilience might be more effectively shared among those with an interest in a successful economy.

Martin McTague
Policy Director

EXECUTIVE SUMMARY

The importance of small businesses and the digital economy

Smaller businesses make up the overwhelming majority of the UK's business population. It is in small businesses that most of the UK's private sector workforce is employed. Small businesses create more new jobs than larger businesses. They also contribute the majority of both private sector employment and employment creation in the UK. Consequently, small businesses are vital to the future success of the UK's economy.

The spread of digital technology offers smaller businesses a number of opportunities to thrive. Small firms are looking to take advantage of these opportunities as effectively as possible by embracing new information technology. Such technology can reduce operating costs, play a central role in increasing productivity and help small businesses to reach new customers.

Cyber crime poses a significant risk to small businesses

The digital element of the economy does however come with a significant downside – the opportunities for legitimate business are matched by opportunities for criminals to commit increasingly sophisticated and highly lucrative crime. Foreign Governments can also take the opportunity to steal valuable economic assets such as the intellectual property (IP) of small businesses or use small businesses as a route to stealing the IP of larger businesses or to gain access to Government systems.

The costs of these downsides is increasing. FSB's recent survey of crime against small businesses found that:[1]

- Two-thirds (66%) of our members had been a victim of cyber crime.
- The average number of times that small businesses had been a victim of cyber crime over the two years (2014 and 2015), was four.
- Small businesses were the victims of around seven million cyber crimes per year (in 2014 and 2015).
- The average cost of cyber crime against small businesses, over the two-year period surveyed, was £3,000.
- The total annual cost to small business was around £5.26 billion (over 2014 and 2015).

Small businesses face a number of challenges

Cyber threats are growing because of:

- A number of vulnerabilities in the digital communications networks and supply chains which underpin the production and circulation of goods and services to consumers.
- The lucrative profits that can be made by cyber criminals through exploiting these vulnerabilities, with few downside risks.
- The temptation of being able to steal the IP of competitor businesses and achieve a commercial advantage, again with minimal risk.
- The politics of statecraft and the ease with which network and supply chain vulnerabilities enable one Government to spy on the economic activities of rival states.
- The political agenda of 'hacktivists'.

There are two main categories of vulnerabilities which pervade the digital communication networks and commercial supply chains (and which are exploited by cyber criminals) of the economy:

- Organisational vulnerabilities: These are weaknesses in the procedures, processes and human behaviour within a business. These have significant consequences for the security and integrity of the assets of a small business such as financial details and customer data.
- Technological vulnerabilities: These are weaknesses in the technology itself, which can leave those using the technology, such as small businesses, open to attack.

[1] FSB, Business Crime Survey, 2016.

Alongside these vulnerabilities, small businesses operate under a number of inherent resource and knowledge constraints. These include: access to finance capital, a limited internal division of labour, considerable opportunity costs especially in relation to spending time not focussed on meeting customer orders and generating new business, a small asset base and bargaining power limitations due to size. As a result, most do not have access to the resources and knowledge to best develop their business's cyber resilience.

These constraints, along with the technological and organisational vulnerabilities means that small businesses are generally not well placed to reduce their own exposure to cyber risks. Neither are they best placed to contribute significantly to the high level of resilience among the commercial supply chains in which they participate and the digital communication networks on which they rely.

Building cyber resilience will help protect smaller firms

The best way to deal with the risks is by making digital networks and supply chains more resilient. Resilience is, in part, about improving security through increasing protection and prevention. It is also a broader concept. Resilience recognises the reality that:

- Some risk is inevitable in any open system, and the openness that new technology brings is an overall positive for small businesses.
- Risk can be positive because it leaves room for innovation and change.
- Most small businesses will be attacked at some point. Cyber crime is too pervasive for that not to be the case. Therefore, it is vital that a business not only protects itself as much as possible, but on the occasions that protection fails the business can survive the attack and thrive once again afterwards. The same is true of any digital communications network and commercial supply chain. The disruption of a cyber attack has to be effectively and quickly managed and overcome.

How to increase resilience

The interconnected nature of the technological and organisational vulnerabilities, and the constraints within which small businesses operate means they need to be tackled holistically and systematically. A multi-faceted policy response is required.

Underpinning specific policy measures should be an understanding that the approach has to be a shared one, with both the public and private sector taking a share of the responsibility. We welcome the fact that the Government has made this understanding a key part of their strategy to date.

Nevertheless, the burden of responsibility needs to be rebalanced to both reflect the distribution of resources, and who has the capability to deal with the vulnerabilities. It is only through a different balance in responsibilities that the UK will significantly increase its cyber resilience and in turn reduce the number of cyber crimes against the UK small business community and lessen the overall negative impact on commercial activity.

The UK Government has to continue to take a leading role and set the direction for the private sector to follow. It can do this in part by establishing the right policy framework to encourage business to make the right cyber resilience choices. In particular:

- Business providing the technological and economic infrastructure need to be encouraged to bear more of the burden of increasing resilience across the digital networks and commercial supply chains.
- Small businesses need support from the Government to help them make the best decisions about improving cyber resilience.

KEY RECOMMENDATIONS

This report makes eight core recommendations, which we have summarised below. A more comprehensive set of recommendations can be found at the conclusion of the report.

Implementing these proposals should lead to a significant overall increase in the cyber resilience of the UK small business sector and the UK economy.

Minimising organisational vulnerability

- Expand the Cyber Information Sharing Partnership (CISP) with compulsory participation for all large and medium-sized businesses and explore the possibility over the long term of bringing in smaller businesses too.

Reducing technological vulnerability

- Require software providers, especially those providing cyber security software, to make automatic patching and updates the default option on all products. Hardware suppliers, such as providers of wifi routers, should also have to have adequate security features bundled in with their products and a high default protection setting.
- The Government should press ahead with encouraging internet service providers (ISPs) to take a leading role in tackling cyber threats and legislate for a 'back-stop' legal requirement for ISPs. This legislation should address activities such as malware filtering across their networks and improve their overall approach to security.
- The current Innovation Vouchers scheme for cyber security should be significantly expanded, enabling it to be used for a much wider range of resilience enhancing measures.

Better enforcement against cyber criminals

- Law enforcement should have a central place in the UK's National Cyber Security Strategy and should focus enforcement towards protecting business, in particular smaller firms. This should include a commitment to survey and record the scale of cyber crime against the UK's business community more routinely, including as part of the official crime statistics.
- Improve the effectiveness of the reporting channels for victims of cyber crime as well as the end-to-end response to cyber crime and fraud.
- The Government needs to commit more resources to enforcement against cyber crime. This should begin at the start of the next public spending cycle.
- Investment in the police and prosecution services needs to focus on substantially increasing the cyber capability and capacity of police officers, civilian support staff, forensic services and prosecutors.

SMALL BUSINESSES ARE CRITICAL TO THE UK ECONOMY

Small businesses make up 99.3 per cent of all businesses in the UK. They contribute 51 per cent of the UK's GDP and employ 58 per cent of the private sector workforce.[2]

The makeup of the business population illustrates the crucial importance of effective Government policy that supports the small business sector. Five million businesses in the UK are micro-businesses employing zero to nine people. Micro-businesses account for 33 per cent of employment and 19 per cent of total UK business turnover. Small businesses – employing 10-49 people – account for a further 15 per cent of employment and 15 per cent of total UK business turnover. Between 1998 and 2010, existing small businesses created 34 per cent of new jobs while start-ups created a further 33 per cent of new jobs.[3] Overall, over two thirds of net job creation in the period 1998 to 2010 was in small businesses.

Small businesses are important for the economy because:

- They drive competition and as a result increase efficiency within and across sectors.
- They innovate, bringing new goods and services to market.
- They generate employment opportunities.
- They form an integral part of the commercial supply chains which enable consumer focussed businesses to provide goods and services.

The digital economy offers many opportunities for small businesses

The majority of small businesses now participate in the digital economy.[4] The internet is an indispensable tool for a lot of smaller firms.

Ofcom has found that 78 per cent of smaller businesses use a broadband connection and that 97 per cent of these small businesses use email and 89 per cent used it for other types of web access. 83 per cent ordered goods or services online and 39 per cent of small businesses said they also used the internet for marketing purposes.[5]

FSB research similarly found that 88 per cent of FSB members said that access to the internet was important for marketing, 86 per cent for business development, 79 per cent for selling goods and services, and 63 per cent for taking payments.[6]

Utilising information technology brings numerous benefits to small business through:

- Reducing operating costs.
- Enhancing efficiency e.g. through helping introduce new ways of working.
- Enabling access to new markets, which because of distance and other factors, may have previously been hard to reach.
- Facilitating better and more efficient customer and supplier management.

Cumulatively, these benefits help make small businesses more successful. The wider UK economy in turn then benefits from a thriving small business sector.

[2] BIS, Business Population Estimates for the UK and Regions November 2015.
Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/467443/bpe_2015_statistical_release.pdf

[3] BIS, SMEs: the Key Enablers of Business Success and the Economic Rationale for Government Intervention

[4] Ofcom, Broadband services for SMEs: assessment and action plan.
Available at: http://stakeholders.ofcom.org.uk/market-dataresearch/other/telecoms-research/smes-research-jun15/

[5] Ofcom Broadband services for SMEs: assessment and action plan.
Available at: http://stakeholders.ofcom.org.uk/market-dataresearch/other/telecoms-research/smes-research-jun15/

[6] FSB Reassured, Optimised, Transformed: driving digital demand among small businesses. September 2015.
Available at http://www.fsb.org.uk/docs/default-source/Publications/reports/fsb-telecoms-report---september-2015(2).pdf?sfvrsn=0

The risks of the digital economy

The adoption of information communication technology (ICT) across the economy over the last 25 years has bought considerable new risks for both the demand (consumer) and supply (business) side of the economy. The central place that ICT has in virtually all commercial activity today means that these risks are pervasive, touching all those engaged in developing, making, buying and selling goods and services.

These risks are a result of the vulnerabilities of the digital technology that the economy relies upon. The risks are magnified considerably by the deployment of the technology through complex digital networks and as a vital component of the commercial supply chains which constitute the economy.

Information and security arrangements are inherently shared across a network – and pertinently for small business, across a supply chain. The cyber security of any one organisation within this chain is potentially only as strong as that of the other members of the supply chain.

Low levels of resilience across digital networks and supply chains can impose considerable costs on businesses, consumers and the economy. For small businesses, these costs are often significant and can be fatal in some cases. The costs are not confined to the direct financial costs of an attack but are wider, impacting a small business's ability to meet orders, get new customers as well as their online or digital reputation. Businesses connected via the supply chain and/or the wider network can also for example face a financial or reputational cost.

Small business owners are focussed on building and sustaining their businesses. Most do not have the resources or skills to combat current and future cyber threats. For this reason it is crucial that the burden of improving cyber resilience is appropriately shared.

Government cyber policy is moving in the right direction and is ahead of the curve compared to many other countries. FSB welcomes this. However, FSB research shows that cyber crime is a problem that is not going away and is, if anything worsening. FSB calls on the UK Government to go further to protect smaller businesses from cyber threats as this will protect the wider UK economy.

THE SCALE OF THE THREAT, THE QUANTITY OF DAMAGE

The nature of the threat

Threats to the digital economy in general – and small businesses in particular – are significant and growing. They come from a range of sources and take a number of forms.

Perhaps the most prominent source of risk comes from those attempting to commit cyber crime. Cyber crimes are generally agreed to be 'offences that are committed against individuals or groups of individuals using modern telecommunication networks such as internet and mobile phones'.[7]

Cyber crimes can be committed by 'hackers themselves or from computers that have been compromised to serve the hacker's need without the users knowledge (bots)'.[8]

They usually utilise a range of tools and methods. These include:[9]

- Phishing – email scams which are aimed at obtaining personal and financial information from the recipient.[10]
- Spear Phishing – the use of a personalised communication, notionally from someone known to the receiver, to deceptively obtain personal and financial information from the receiver.
- Malware – an umbrella term for many of the most damaging software applications such as trojans, worms,[11] viruses, spyware, ransomware, root kits,[12] key loggers, browser hijackers etc.
- Distributed Denial of Service (DDoS) attacks – inundation of internet traffic from a number of sources which overwhelm systems making them unusable.

The aims of cyber criminals using these tools and methods most commonly include:

- Theft of data, especially of personal information, money and intellectual property.
- Attempts to obtain money or other business assets through deception i.e. fraud, such as card-not-present (CNP) fraud.
- Extortion, against both businesses and their customers.

Other threats include:

- Corporate espionage by rival businesses seeking a company's IP.
- Cyber espionage by foreign Governments.
- 'Hacktivists' looking to convey political messages and pursue a political agenda by damaging the integrity and operability of certain technologies or organisations.

The target of these threats can include:

- Governments.
- Businesses (large and small and of all types, in all sectors including those who provide the economic infrastructure for the economy such as banks).
- Households.
- Digital infrastructure.

[7] Britz cited in. Wori, O, Computer Crimes: Factors of Cyber criminal Activities, International Journal of Advanced Computer Science and Information Technology, Volume 3, Issue 1, 2014.

[8] Parliamentary Office of Science and Technology, Cyber Security in the UK, 2011.

[9] Parliamentary Office of Science and Technology, Cyber Security in the UK, 2011.

[10] 'Vulnerability to low-level attacks such as phishing can compromise information that can then be used in large scale attacks'. Source: Parliamentary Office of Science and Technology, Cyber Security in the UK, 2011.

[11] Worms are '...a subset of malware able to spread and replicate across a network or through removable media'. Source: Parliamentary Office of Science and Technology, Cyber Security in the UK, 2011.

[12] Root kits are '...software to gain and maintain privileged access to computer systems; can be used to conceal other malware'. Source: Parliamentary Office of Science and Technology, Cyber Security in the UK, 2011.

Types of cyber crime felt by smaller businesses by sector

For small businesses:

- FSB research shows that Phishing[13] and Spear Phishing[14] are the most common types of cyber attack, experienced by 49 per cent and 37 per cent of respondents respectively.[15]
- Malware attacks were the third most reported type of cyber attack, experienced by 29 per cent of respondents. FSB research found that 10 per cent of small businesses had suffered from CNP fraud.[16]

Table one: Types of cyber crimes reported by key sectors
Source: FSB Business Crime Survey 2016

	All sectors	Manufacturing	Construction	Wholesale and retail trade; repair of motor vehicles and motorcycles	Transportation and storage	Accommodation and food service activities	Information and communication	Financial and insurance activities	Professional, scientific and technical activities	Administrative and support service activities	Arts, entertainment and recreation
Phishing	49%	55%	45%	47%	52%	38%	38%	43%	57%	51%	68%
Spear Phishing	37%	41%	41%	32%	43%	28%	28%	44%	43%	41%	51%
Malware attack	29%	34%	20%	22%	28%	24%	28%	35%	38%	33%	21%
Card not present fraud	10%	10%	9%	21%	14%	16%	4%	4%	4%	10%	8%
Denial of Service Attack	5%	4%	1%	4%	4%	4%	13%	5%	3%	10%	3%
Ransomware attack	4%	7%	1%	2%	0%	2%	7%	0%	1%	10%	3%
Online intellectual property theft	3%	6%	1%	2%	3%	0%	7%	0%	2%	0%	11%
Online invoice fraud	3%	5%	5%	4%	5%	2%	6%	0%	1%	4%	0%
Identity theft of owners/ employees/ business	3%	3%	3%	3%	0%	2%	4%	0%	2%	7%	7%
Online corporate identity fraud i.e. website cloning	2%	2%	1%	1%	3%	2%	3%	0%	1%	4%	0%

[13] Phishing describes the use of electronic communications channels to attempt to deceptively obtain personal and financial information from the receiver.

[14] Spear Phishing describes the fraudulent use of electronic communication, like Phishing, but the relevant email appears to be someone or an organisation the receiver knows.

[15] FSB, Business Crime Survey, 2016.

[16] Fraudulent use of a payment card such as a credit card where the card is not physically presented to the merchant, rather payment takes place at a distance e.g. online.

Unsurprisingly, different crimes were distributed differently between sectors. Table one illustrates how different sectors are impacted by different types of cyber crime.

KEY RESULTS:

- Reporting of Phishing and Spear Phishing attacks was generally high across all sectors, but both types of Phishing had the highest incidence in the arts, entertainment and recreation sector.[17]
- Malware was most prevalent against the manufacturing, finance and insurance, professional services and administrative and support services sectors.[18]
- The proportion of businesses in the wholesale, retail and motor repair sectors that had been a victim of CNP fraud was double the proportion reporting CNP fraud across all sectors, with nearly 21 per cent of respondents suffering from it. Just behind the wholesale, retail and motor repair sector are the transportation and storage sector and accommodation and food service sectors. These are all generally consumer facing sectors, where the opportunities for the fraudulent use of credit cards and other payment systems is high.[19]
- IP theft was reported by over one in ten of respondents in the arts, entertainment and recreation sector.
- DDoS[20] and ransomware[21] attacks were noticeably higher in both the information and communications and the administrative and support services sectors.

[17] These levels of reporting should not be surprising. As the latest Threat report from Symantec shows, 1 in every 1,846 emails sent in 2015 was a Phishing email. Symantec identified 1,305 Spear Phishing campaigns in 2015, each involving on average, 12 email attacks, against 11 recipients over a 6 day period. Source: Symantec, Internet Security Threat Report: Volume 21, 2016.

[18] Symantec have identified that around 1 in 220 emails sent and received in 2015 was infected with malware and that one in 3,172 websites were infected with malware in 2015. 431 million new malware variants were added to the internet in 2015. For mobile devices there were 3,944 new variants of malware created. Source: Symantec, Internet Security Threat Report: Volume 21, 2016.

[19] The UK Cards Association identified 1,019,146 remote purchase (i.e. Card Not Present) frauds in 2014. This equated to a cost of around £331,500,000 in 2014. Incidents were increased from 875, 086 in 2008, including a seven per cent increase between the years 2013 (951, 988) and 2014. In value terms Card Not Present frauds increased by 10 per cent between 2013 and 2014. The trend is one of steep annual increases. It is no surprise therefore that consumer facing businesses in particular are suffering at around twice the average for all the sectors FSB surveyed. Source: UK Cards Association, Card fraud figures, 2016.
Available at: http://www.theukcardsassociation.org.uk/plastic_fraud_figures/

[20] These levels of reporting should not be surprising. The latest 'Threat' report from Symantec shows that in 2015 there were 362,000 Crypto-ransom-ware attacks. That is 992 per day for the whole of 2015. This was an increase of 35 per cent on the numbers of incidents in 2014. Source: Symantec, Internet Security Threat Report: Volume 21', 2016.

[21] Symantec described the trend in Denial of Service (DDoS) Attacks as '...growing in intensity and frequency. For example, Symantec saw a 183 percent increase in DNS amplification attacks between January and August 2014. According to a survey by Neustar, 60 per cent of companies were impacted by a DDoS attack in 2013 and 87 per cent were hit more than once. Motives include extortion for money, diversion of attention away from other forms of attack, hacktivism, and revenge. Increasingly, would-be deniers of service can rent attacks of a specified duration and intensity for as little as $10–$20 in the online black market'. Source: Symantec, Internet Security Threat Report 20, 2015.
In September 2015 alone, Symantec identified over 15 million DDoS attacks. Source: Symantec, Internet Security Threat Report: Volume 21, 2016.

Types of cyber crime and business size

FSB research also suggests that certain types of cyber crime are more associated with businesses of a particular size.

Table two: Type of cyber crime reported by business size
Source: FSB Business Crime Survey 2016

	No employees	Up to 10 employees	11-20 employees	21-50 employees	51+ employees
Phishing	49%	49%	44%	49%	54%
Spear Phishing	38%	38%	30%	34%	49%
Malware attack	22%	31%	28%	37%	40%
Card not present fraud	5%	10%	17%	12%	18%
Denial of Service Attack	4%	6%	3%	4%	6%
Ransomware attack	2%	3%	6%	15%	5%
Online intellectual property theft	3%	2%	2%	9%	6%
Online invoice fraud	3%	3%	3%	0%	7%
Identity theft of owners/ employees/ business	0%	4%	1%	7%	6%
Online corporate identity fraud i.e. website cloning	0%	2%	2%	4%	7%

Some of the more notable variances in the distribution of cyber crimes between the different sizes of businesses include:

- Spear Phishing is less prevalent amongst businesses with between 11 and 20 employees.
- Malware attacks appear to be more common against those with up to 10 employees and those with 21 or more employees.
- Medium-sized businesses reported being subject to CNP fraud significantly more than micro-businesses. The proportion of incidents against the former were on a par with those suffered by businesses with between 11 and 20 employees.
- Ransomware attacks were noticeably more frequently reported by those businesses in the 21 to 50 employees range. This group was also most likely to report being a victim of IP theft.
- Medium-sized businesses suffered from website cloning and other business identify theft issues.

Types of cyber crime and the number of reported cases by smaller firms

A more detailed look at the distribution of the different types of cyber crime among those reporting themselves as victims does not alter the distribution of cyber crime types. However, it does give a further indication of the rates at which those who are victims of cyber crime are suffering from it.

Table three: Distribution of cyber crime among the victims
Source: FSB Business Crime Survey 2016 and BIS Business Population Estimates

Types of cyber crime	Proportion of respondents reporting being a victim
Phishing	74%
Spear Phishing	56%
Malware attack	44%
Card not present fraud	15%
Denial of Service Attack	7%
Ransomware attack	6%
Online intellectual property theft	4%
Online invoice fraud	4%
Identity theft of owners/ employees/ business	3%
Online corporate identity fraud i.e. website cloning	2%

Of those reporting themselves as a victim the data shows:

- Three-quarters (74%) suffered from Phishing attacks.
- Over half (56%) experienced a Spear Phishing attack.
- 44 per cent were victims of malware attacks.
- Nearly 15 per cent suffered from CNP fraud.
- Seven per cent were subject to their website being attacked and customers prevented from accessing it through a denial of service attack.
- Six per cent were subject to ransomware attacks.

The overall scale of cyber crime against UK small businesses

At a global level, Symantec identified that over 400 million identities were 'exposed' due to cyber breaches in 2015.[22] The Centre for Strategic and International Studies and McAfee have estimated that cyber crime and cyber espionage together cost the global economy somewhere between $375 billion and $575 billion a year. The exact figure depends on the particular methodology employed.[23] Even at the lower end of the range these figures represent significant sums of money being stolen by criminals, making cyber crime a highly lucrative 'industry'.

[22] Symantec, Internet Security Threat Report: Volume 21, 2016.

[23] McAfee acknowledges in the report that there is a lack of accurate data but, the current attempts at estimating the scale of cyber crime '...until reporting and data collection improve...provide a way to estimate the global cost of cyber crime...'. Source: Centre for Strategic and International Studies and McAfee, Net Losses: Estimating the Global Cost of Cyber crime: Economic Impact of Cyber crime II, 2014.

The scale of cyber crime suffered by UK small businesses

FSB research shows estimates the scale of the problem specifically faced by the UK's small and medium sized business population is alarming. Two thirds (66%) of FSB members across the UK reported being a victim of cyber crime in the two years 2014 and 2015.[24] The average number of times a member business had been a victim of cyber crime over the same period was four.[25]

Together, the proportion of respondents who were victims combined with the frequency of victimhood over the two year period surveyed, suggests that in the UK, small businesses were on average the victims of around seven million cyber crimes a year in 2014 and 2015.[26]

Table three breaks down the 'two-thirds of respondents had been victims' figure into the types of cyber crimes of which they had been victims of. Table four below illustrates the proportion of respondents by sector, who had not been victims of cyber crime over the two year period 2014 and 2015.

Not all small businesses are victims of cyber crime

Table four: Respondents reporting they were not a victim of cyber crime by sector
Source: FSB Business Crime Survey 2016

	Manufacturing	Construction	Wholesale and retail trade; repair of motor vehicles and motorcycles	Transportation and storage	Accommodation and food service activities	Information and communication	Financial and insurance activities	Professional, scientific and technical activities	Administrative and support service activities	Arts, entertainment and recreation
Not a victim of cyber crime	27%	36%	31%	26%	37%	41%	40%	28%	23%	14%

The three sectors where the overall incidence of cyber crime was found to be the lowest were the information and communications sector; the accommodation and food services sector; and the financial and insurance sector.

In contrast, the arts, entertainment and recreation sector reported the least amount of cyber crimes. This is perhaps unsurprising. If you are a business supplying 'cultural' services then the internet is a vital tool for advertising your services and in some cases delivering them too. Therefore, the digital presence of a business in this sector is likely to be high, making it a likely target.

Data collected by FSB, and outlined in Table five suggests that:

- The very smallest businesses were somewhat less likely to be a victim of a cyber crime than those businesses in the middle of the small and medium-sized (i.e. 11 to 20 employee) business range.
- The category of business with the highest proportion reporting that they were victims of cyber crime was the medium-sized sector.

[24] The approximate two-thirds figure excludes those who responded Don't Know to the questions about whether they had been victim of cyber crime in the preceding two years. Source: FSB, Business Crime Survey, 2016.

[25] FSB, Business Crime Survey, 2016.

[26] Calculation made using FSB survey data collected in January 2016 and BIS business population estimates. Source: BIS/ National Statistics, Business Population Estimates for the UK and Regions 2015.
Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/467443/bpe_2015_statistical_release.pdf
According to BIS's latest business population data there are 5.4 million businesses in the UK, approximately 5,362,200 are SMEs. The survey found two-thirds of SMEs surveyed had been victims of at least one cyber crime over the preceding two years. Extrapolated across the UK, this suggests that 3,539,052 SMEs had been a victim of cyber crime in the last two years. FSB survey data suggested the average number of times a business has fallen victim is four. Suggesting that the levels of victimhood of cyber crime, among the UK's small and medium-sized business community, could be as high as 14,156,208 crimes. Dividing that two year number by the number of years gives an average of 7,078,104 cyber crimes per year.

However, the disparities in the size categories should not distract from the fact that even among the smallest levels of victimhood are high e.g. for the smallest category, just under two-thirds were victims.

Table five: Businesses reporting that they had not been a victim of cyber crime in the preceding two years by size[27]
Source: FSB Business Crime Survey 2016

	No employees	Up to 10 employees	11-20 employees	21-50 employees	51+ employees
Not been a victim of cyber crime	37%	29%	32%	19%	13%

The chances of even the self-employed / no employee businesses falling victim to cyber crime are considerable. In fact, the self-employed are only eight per cent less likely to be a victim than a micro-business of 10. Further, there is not a clear relationship between size and victimhood as businesses of between 11 and 20 employees are less likely to be a victim than businesses with up to 10 employees.

The risks of a cyber attack are getting worse

Attackers are becoming more effective, while victims are getting less good at discovering attacks. This signals a worsening situation. Research by Verizon found that, while in 60 per cent of cases it takes minutes to successfully breach an organisation's information technology there is '…a growing 'detection deficit' between attackers and defenders'.[28] Trustwave's latest Global Security Report found that the median length of time between 'intrusion' into a system and 'detection' was 80.5 days.[29] It took a further two days for 'containment'.

After a breach has been discovered, the recently published 'Cyber Security Breaches Survey 2016' found that:[30]

- Small businesses (i.e. those with less than 50 employees) needed 2.2 days on average to recover from an information breach.
- For medium-sized businesses the average was also 2.2 days.

Notably it took: "…micro firms slightly longer to recover from a breach, with a quarter…saying it took up to a week to recover from their most disruptive breach".[31]

The costs of cyber crime to small businesses

The average cost of cyber crime to small businesses was just under £3,000.[32] The impact of an attack for the smallest businesses is likely to be greater than for a medium-sized business. For many of the former, £3,000 could be the difference between making a profit or a loss in a business quarter or half year period. For a start-up the impact could be even greater. A cyber attack costing around £3,000 could wipe out their working capital and result in the start-up going out of business before it has had a chance to grow.[33]

[27] Percentages in this table have been rounded to the nearest whole number.

[28] Verizon, 2015 Data Breach Investigations Report, 2015.

[29] Trustwave, Trustwave Global Security Report, 2016. Available at: https://www2.trustwave.com/rs/815-RFM-693/images/2016%20Trustwave%20Global%20Security%20Report.pdf

[30] Klahr, R et al, Cyber Security Breaches Survey 2016: Main Report, 2016.

[31] Klahr, R et al, Cyber Security Breaches Survey 2016: Main Report, 2016.

[32] FSB, Business Crime Survey, 2016.

[33] FSB, Business Crime Survey, 2016.

The data collected through FSB's Business Crime Survey, suggests that the level of financial detriment for small businesses due to cyber crime is likely to be in the region of £5.26 billion a year.[34] This is a significant burden on the small business sector.

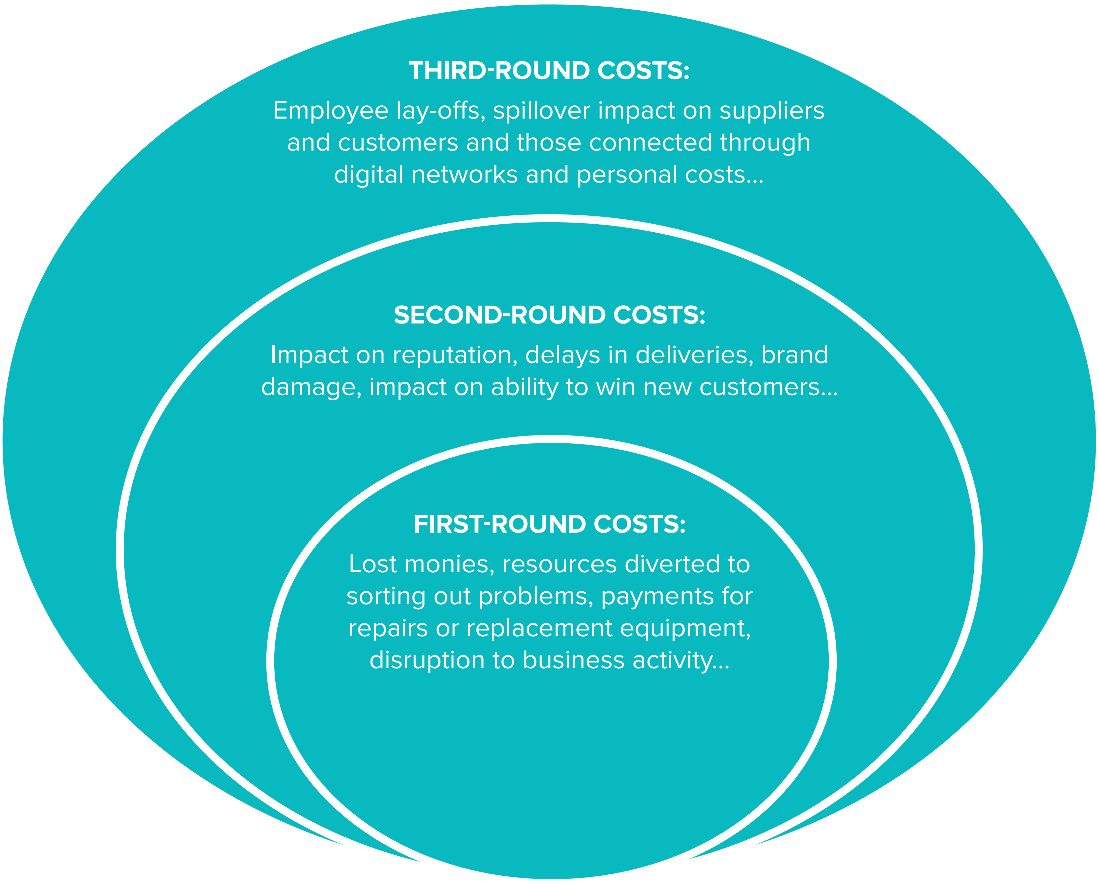
The evidence suggests a good deal of ongoing detriment already. Furthermore, many expect the situation to worsen before any improvements are seen.

> "…as more business activities move online and as more consumers around the world connect to the internet, and as autonomous devices are connected ('the Internet of things'), the opportunities for cyber crime will grow. Cyber crime remains a growth industry".[35]
>
> Centre for Strategic and International Studies and McAfee, Net Losses; Estimating the Global Cost of Cyber Crime

Breaking down the impact of a cyber attack

The costs of a cyber attack can be broken down into three categories. These are illustrated in diagram one below.

Diagram one: Categories of costs of a cyber crime


THIRD-ROUND COSTS:
Employee lay-offs, spillover impact on suppliers and customers and those connected through digital networks and personal costs…
SECOND-ROUND COSTS:
Impact on reputation, delays in deliveries, brand damage, impact on ability to win new customers…
FIRST-ROUND COSTS:
Lost monies, resources diverted to sorting out problems, payments for repairs or replacement equipment, disruption to business activity…

As diagram one shows, there is a ripple effect beyond the initial successful attack that multiplies the costs for the victim's business and those they are connected to through supply-chains and digital networks. Each successful attack therefore results in numerous rounds of costs, not just those which the small business initially suffers.

[34] Multiplying the average cost of cyber crime as reported by the respondents to FSB's 'Business Crime Survey' by the proportion of SMEs who had been a victim of cyber crime over the two year period 2014 and 2015 (according to FSB's survey responses) then total cost to the SME community for that period is in the order of: £10,532,218,752. Dividing this by the number of years respondents were questioned about, gives an average figure per year of £5,266,109,376.

[35] Centre for Strategic and International Studies and McAfee, Net Losses; Estimating the Global Cost of Cyber crime, 2014.

In the first instance, there are the most obvious costs:

- Money stolen.
- Money defrauded.
- Funds extorted.
- Paying to repair and replace attacked IT and related equipment.[36]

In addition to the very direct list of costs outlined above is the likely negative impact on the ability of the business to operate as efficiently and effectively as it would under normal conditions.[37]

The Ponemon Institute has created a breakdown of the costs of an attack. Their breakdown offers an indication of the different costs that can be incurred when a small or medium-sized business is the victim of a cyber crime.[38]

The Ponemon research found that:[39]

- Around 39 per cent of the costs to a business is 'business disruption'.
- Approximately 35 per cent is 'information loss'.
- 21 per cent is 'revenue loss'.
- Four per cent is 'equipment damage'.

Research by Ipsos-Mori found similarly high numbers of respondents reporting the disruptive impact on business activity:[40]

- 42 per cent of business respondents said that the information breach required 'additional staff time to deal with the breach'.
- 31 per cent said the successful breach 'stopped staff carrying out day-to-day work'.

Each on its own would have productivity implications. The combination of the two types of disruption suggests a considerable negative impact on the productivity of those businesses who suffer from cyber crime.

Further, the revenue impacts for micro-businesses in particular are noticeably higher than for other sized businesses. Ipsos-Mori identified that 18 per cent of micro-businesses suffered lost revenues due to information breaches.[41] This is close to the 21 per cent identified by the Ponemon Institute.

A range of 'second-round-costs' beyond the immediate direct financial costs of being the victim of a successful cyber attack can also be identified. These include:

- Delays in delivery.[42]
- Negative impact on the reputation of the business.[43]
- Damage to the business's brand.[44]

[36] 55 per cent of businesses reported that a key impact of an information breach was the need to purchase new security measures to prevent future attacks. While 23 per cent reported there were other repair and recovery costs due to the information breaches they suffered. Source: Klahr, R et al (2016). 'Cyber Security Breaches Survey 2016'.

[37] 93 per cent of small business that had been a victim of a cyber breach surveyed by KPMG for Cyber Streetwise said that being a victim of a cyber attacks impacted the business' ability to operate. Source: KPMG/ Cyber Streetwise, Small Business reputation and the Cyber Risk, 2015. Available at: https://home.kpmg.com/content/dam/kpmg/pdf/2016/02/small-business-reputation-new.pdf

[38] It should be noted that the sample size was relatively small and international and consequently not strictly representative of the UK's business population. The Institutes figures should therefore be taken as an indication of what could be the case in UK businesses.

[39] Ponemon Institute, 2015 Cost of Cyber Crime Study: Global, 2015. Available at: http://www.cnmeonline.com/myresources/hpe/docs/HPE_SIEM_Analyst_Report_-_2015_Cost_of_Cyber_Crime_Study_-_Global.pdf

[40] Klahr, R et al, Cyber Security Breaches Survey 2016: Main Report, 2016.

[41] Klahr, R et al, Cyber Security Breaches Survey 2016: Main Report, 2016.

[42] 26 per cent of small business that had suffered a cyber breach surveyed by KPMG for Cyber Streetwise said that being a victim of a cyber-attacks caused customer delays. Source: KPMG/ CyberStreetwise, Small Business reputation and the Cyber Risk, 2015. Available at: https://home.kpmg.com/content/dam/kpmg/pdf/2016/02/small-business-reputation-new.pdf
The Cyber Security Breaches Survey 2016 found that 12 per cent of those reporting breaches were unable to provide their goods and/ or services to customers as a result of the breach. Source: Klahr, R et al (2016). 'Cyber Security Breaches Survey 2016'.

[43] A KPMG/ Cyber Streetwise survey found that of those small businesses surveyed and had suffered a cyber breach 89 per cent felt that their business's reputation had been negatively impacted. Source: KPMG/ Cyber Streetwise, Small Business reputation and the Cyber Risk, 2015. Available at: https://home.kpmg.com/content/dam/kpmg/pdf/2016/02/small-business-reputation-new.pdf

[44] 31 per cent of small business surveyed by KPMG for Cyber Streetwise said that being a victim of a cyber attacks had damaged their brand.

- Loss of existing customers.[45]
- Hindrances to winning new business.[46] [47]
- Obstacles to recruiting new employees.

Any one of these impacts can be damaging to a small business. Their size, availability of labour and small customer base means that smaller businesses find it difficult to rescue a brand once it has been damaged.

For one in ten businesses, the damage can be so significant that they are unable to keep their business operating in the same sector and have to change the nature of their business.[48] Consequently, it is fair to argue that cyber risks can alter the very structure of the UK economy.

There are also 'third-round' costs. These can range from a business being forced to lay off workers because of the long-term impact on profits to the ripple effect through the supply chains in which the victim business is part of. The interconnected nature of modern supply chains can result in the suppliers and customers of the original victim business also bearing considerable costs which in turn impact their other suppliers and customers. These costs might come about for a number of reasons:

- Exposing customers and suppliers to the risk of a similar attack.
- The knock-on effects for those who are unable to receive a good or service they have perhaps paid for in advance and planned to utilise because of the delays in production and delivery as a result of a cyber attack.
- Inability to make or receive payments from customers and / or suppliers.

These effects can last for considerable periods of time, especially if attacks are not discovered for an extended amount of time.[49] The impact of undiscovered cyber attacks can lead to ongoing negative impacts not only for the original victim but also for customers and suppliers. These wider effects make it harder to measure the exact scale of the attack and its impact on a smaller firm and in turn the wider economy.

Cyber crime also imposes a personal cost. Crimes against smaller firms are every bit as personal as a crime against a household. A crime against a smaller business should not, as they often are, be seen as impersonal and be seen as attack against an entity rather than a person. Smaller firms have often taken considerable risks and challenges to set up and build their. These include:

- Leaving secure employment and benefits such as pensions.
- Risking existing assets to acquire finance to start and run their business.
- Sacrificing time with friends and family.

Finally, in the worst case scenario, a small business could be made insolvent as a result of a successful attack.

Conversely, although still damaging, larger businesses are typically better equipped at dealing with the negative consequences of a cyber attack. Larger firms have the resources and reserves, including a higher number of staff with the necessary skills, and market power to allow them to 'ride out' the cyber attack.

[45] 30 per cent of small businesses that had suffered a cyber breach surveyed by KPMG for Cyber Streetwise said that being a victim of a cyber attacks had led to the loss of clients. Source: KPMG/ Cyber Streetwise, Small Business reputation and the Cyber Risk, 2015.
Available at: https://home.kpmg.com/content/dam/kpmg/pdf/2016/02/small-business-reputation-new.pdf

[46] 29 per cent of small business that had suffered a cyber breach surveyed by KPMG for Cyber Streetwise said that being a victim of a cyber attacks had damaged their ability to win new business .Source: KPMG/ Cyber Streetwise, Small Business reputation and the Cyber Risk, 2015.
Available at: https://home.kpmg.com/content/dam/kpmg/pdf/2016/02/small-business-reputation-new.pdf

[47] Four per cent of respondents to the Ipsos-Mori 'Cyber Security Breaches Survey 2016' who had suffered a security breach identified the fact that they were discouraged from carrying out intended future business activity. Source: Klahr, R et al (2016). 'Cyber Security Breaches Survey 2016'.

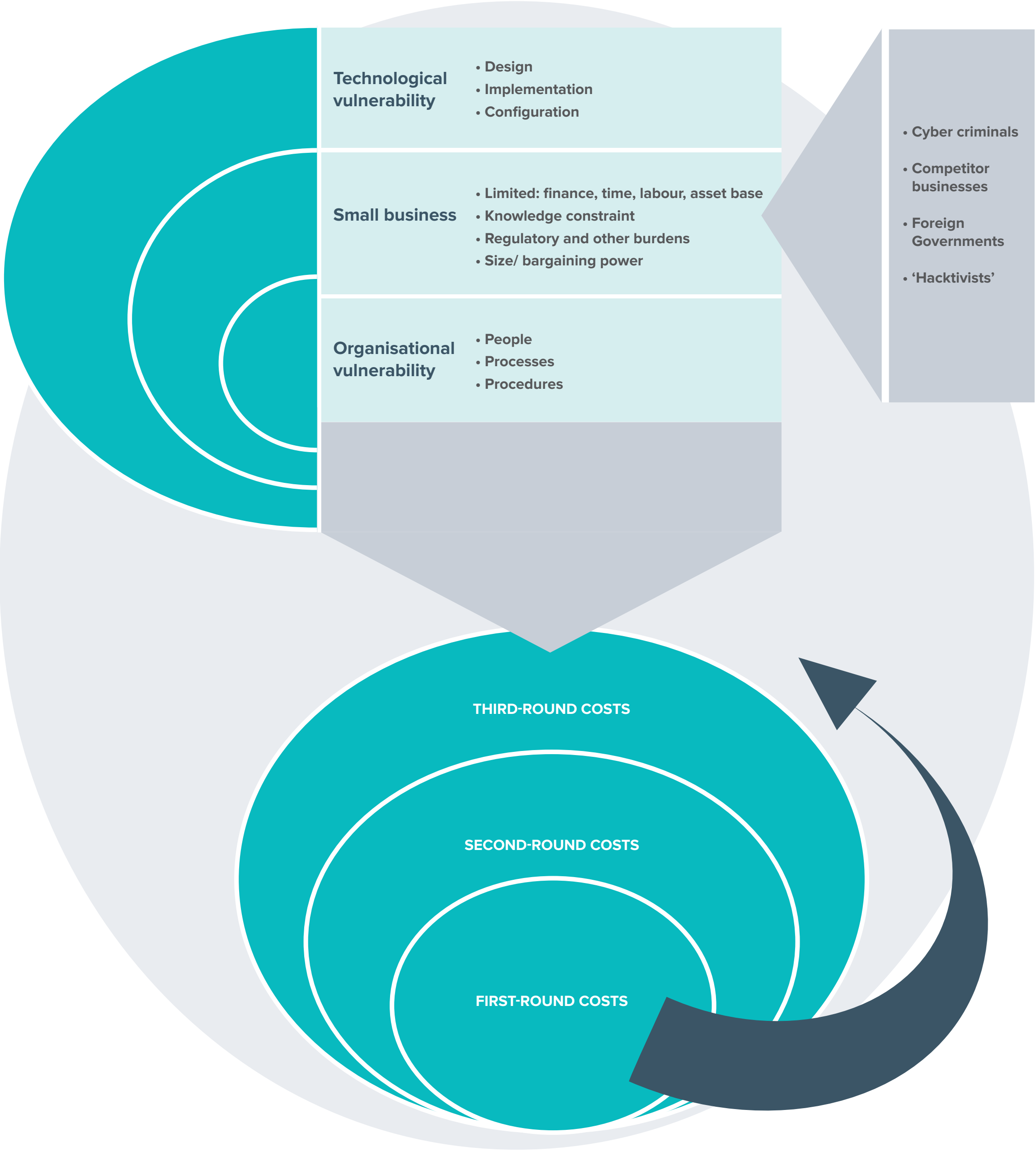
[48] HMG/ PwC, 2015 Information Security Breaches Survey: Executive Summary, 2015.

[49] 22 per cent of respondents to research carried out by Verizon said that they did not manage to contain [breaches] they experienced for months or even years. Source: Verizon DBIR cited in Symantec, A manifesto for cyber resilience, 2014.
Available at: http://www.symantec.com/content/en/us/enterprise/other_resources/b-a-manifesto-for-cyber-resilience.pdf

THE CAUSES OF VULNERABILITY

Both technological and organisational vulnerabilities cause issues for businesses of all sizes. However, the problems are particularly pronounced for smaller businesses. The latter operate under inherent resource and knowledge constraints. These constraints are present in almost all aspects of their business activity, but are particularly salient when it comes to complex risk issues associated with cyber threats and cyber resilience. These constraints have a significant impact on how small businesses interact with ICT and in turn the risk that they generate.

Diagram two: Vulnerabilities exacerbated by the constraints faced by small businesses



Technological vulnerability
- Design
- Implementation
- Configuration

Small business
- Limited: finance, time, labour, asset base
- Knowledge constraint
- Regulatory and other burdens
- Size/ bargaining power

Organisational vulnerability
- People
- Processes
- Procedures

- Cyber criminals
- Competitor businesses
- Foreign Governments
- 'Hacktivists'

Negative ('chilling') impact on the economy

Diagram two above indicates how, in a simplified form, technological vulnerabilities, the constraints on small businesses and organisational vulnerabilities interact. It also illustrates how the intrusion into the 'mix' of vulnerabilities and small business constraints by cyber criminals can lead to a weaker, less productive and dynamic small business sector and economy. This is due to the 'chilling effect' that generally increased levels of risk can have on the incentives for economic activity.[50]

Technological vulnerability sits at the top of the diagram. It shapes the world of small business, in much the same way as it shapes the economy as a whole. Technological vulnerabilities and organisational vulnerabilities can reinforce each other, making the overall vulnerabilities in the system (i.e. the digital networks and commercial supply chains) more than the sum of their parts.

The extent to which the technological vulnerabilities can be mitigated by organisational factors such as having highly expert people in place and effective processes and procedures to reduce the potential impact of technological vulnerabilities, will depend on the resources available to the relevant organisation or organisations. These will necessarily be limited for smaller firms. Consequently, the ability of small firms to optimise their organisational response and mitigate some of the technological vulnerabilities will nearly always fall short.

As diagram two shows, the interconnected nature of the networks and supply-chains pose an additional complication for a modern interconnected economy, in that any weakness in the technology of one business or their staff, processes and procedures comes with a potential negative spill over for other businesses and customers.

The technology vulnerability

The different technologies which enable the formation of digital networks and commercial supply chains, which rely on those communication networks, contain a large number of vulnerabilities. An indication of the extent of these vulnerabilities has been given by Symantec in their latest 'Internet Security Threat Report':[51]

- 78 per cent of the popular websites it scanned in 2015 contained vulnerabilities. 15 per cent had vulnerabilities that were 'critical'.
- 528 vulnerabilities were identified in mobile applications in 2015, an increase of 214 per cent. 3,944 new malware variants for Android mobile operating system were discovered.
- Ransomware increased by 35 per cent in 2015.
- There were 1.1 million bot nets and 431 new malware variants identified.
- A new zero-day vulnerability emerged every week (on average) throughout 2015.[52]

There are three types of technological vulnerability:

1. Design: a weakness in the system or product at an early stage of development.
2. Implementation: a weakness introduced at the stage of putting a design into effect. This can negate a well-designed system.
3. Configuration: a weakness which occurs as a result of the way the system is arranged to operate.

Much of the technological infrastructure contains weaknesses from at least one of these categories, and often more than one. Within each category there are typically a wide range of weakness types. Vulnerabilities in software for example '...are commonly introduced...due to poor programming practice'.[53] Programming decisions are frequently not taken based on the most secure option but on 'other' criteria:[54]

- A programme that a developer is more familiar.

[50] A 'chilling effect' describes the inhibition or discouragement of a certain activity or activities by individuals/ organisations.

[51] Symantec, Internet Security Threat Report: Volume 21, 2016.

[52] A Zero-day vulnerability is a hole in software not known to the vendor. They are often exploited by cyber criminals.

[53] Parliamentary Office of Science and Technology, Cyber Security in the UK, 2011.

[54] White Hate Security, Website Security Statistics Report, 2014.

- Market fashion.
- Speed and cost.
- Available programmer skills sets.
- The options most likely to deliver on time.

This approach to development has been prevalent throughout the history of the development of information and communications technology. Providers of the infrastructure face a number of incentives which drive developers and other infrastructure providers to operate in this way: [55]

- Network effects mean that the value of a product is dependent on how many others use it.
- The cost of the first unit of production, i.e. the software package, is high costing hundreds of thousands, often millions but the cost of producing multiple copies for users is small, making the development of much information and communication technology a high fixed cost, low marginal cost industry.
- There can be a considerable degree of 'lock-in' associated with particular technologies, with users finding it difficult to switch technologies.

> "All three of these effects tend to lead to 'winner take all' market structures with dominant firms. So it is extremely important to get into markets quickly... Once in a vendor will to appeal to complementary suppliers... Once the customers have a substantial investment in complementary assets, they will be locked in".[56]
>
> Anderson, R, Why Information Security is Hard – An Economic Perspective

A further driver has been the need for interoperability, which inevitably means greater openness and vulnerability. Useability is also a factor with some technologies becoming dominant, not because they are the most secure but because they are the easiest to use.

The result of this approach has been that digital information and communication technologies in general and the internet in particular has evolved over many years with little planning or thought for security. This has tended to be an afterthought following the development of a particular technology. It is highly unlikely that Government and individuals will agree to re-build the existing international communications networks in order to make it a more robust system.[57] This means resilience improvements need to be retro-fitted into the existing architecture.

This has remained the situation for so long because those doing the developing and providing the technological infrastructure rarely bear any or much of the cost of the security vulnerabilities in their systems. There is little incentive for them to improve on the current business model.

For small businesses, technological vulnerabilities present a wide range of risks. Not least due to the weaknesses they create in parts of the digital infrastructure that support the provision of essential economic services, such as banking and payment systems. There is good evidence to suggest that many of those providing critical economic infrastructure are not cyber resilient.[58] The latest data from UK Cards Association shows that:[59]

- There were over 53,000 online banking frauds in 2015 (up 26 per cent on the previous year) worth £60.5 million, which in value terms equated to a staggering 48 per cent increase on 2013.
- Gross fraud losses on UK issued cards were over £400 million in 2014, up 6 per cent on 2013.

[55] Anderson, R, Why Information Security is Hard – An Economic Perspective. Available at: https://www.acsac.org/2001/papers/110.pdf

[56] Anderson, R, Why Information Security is Hard – An Economic Perspective. Available at: https://www.acsac.org/2001/papers/110.pdf

[57] Singer, P W and Friedman A, Cyber Security and Cyber War: what everyone needs to know, 2014.

[58] 'Many banks, and other companies for that matter, are failing to do some of the basics to protect themselves from cyber criminals. The elderly technology still used by many banks presents a particular security problem. It is well-known that some banks' legacy technology and applications are 25 or 30 years old, and are therefore difficult to fix and protect. 99 per cent of breaches used old vulnerabilities that governments, banks and companies failed to patch'. Source: Coburn N et al, Cyber crime: The Fast Moving Menace, 2014. Available at: https://risk.thomsonreuters.com/sites/default/files/GRC01950.pdf
The British Bankers Association identified: malware, social engineering, deployment techniques and botnets as particularly common techniques used against banks. Source: BBA and PWC, The Cyber Threat to banking: A Global Industry Challenge. Available at: https://www.bba.org.uk/wp-content/uploads/2014/06/BBAJ2110_Cyber_report_May_2014_WEB.pdf

[59] UK Cards Association, Card fraud figures, 2016. Available at: http://www.theukcardsassociation.org.uk/plastic_fraud_figures/

- Fraud losses on e-commerce were approximately £217 million in 2014 from a total of £331.5 million in losses from CNP fraud.
- The monetary value of ID theft using UK issued cards stood at £29.9 million in 2014, from 26,542 incidents.

These figures are not the hallmark of a secure payments infrastructure. Many of those who provide the key economic infrastructure do not bear much of the cost of those weaknesses when cyber criminals exploit them. Yet, most of the infrastructure providers are sufficiently well-resourced, unlike most small businesses, to better protect their systems. Given the resources at their disposal larger financial intermediaries should take more of a role in plugging these vulnerabilities in ICT and therefore reducing the risk of a cyber crime from taking place.

The constraints on small businesses: why small businesses are vulnerable to technological and organisational weaknesses

Smaller firms should be thought of in the same way as individual consumers across a range public policy issues. This is particularly true with regards to cyber crime.[60]

Small businesses do not have access to the financial, technical and human resources that larger businesses have. Owners of smaller firms often have to act as the CEO, CFO, HR manager, marketing manager, regulatory compliance officer and the sales person. They operate under a number of constraints tied to their size such as:

- Limited asset base and access to financial capital whether internal or external.
- A lack of technical knowledge about cyber issues and a broader awareness and understanding of the possible threat and difficulty in accessing adequate and useable information.
- Considerable opportunity costs of the owner’s limited time, which is focussed on fulfilling orders and finding new business.
- A much more limited internal division of labour, inhibiting the ability to allocate specialist roles outside the core activities of the business.
- Less elaborate governance arrangements than those found in larger businesses.
- Reduced bargaining power in relation to other larger parties.

These constraints have two effects, which can result in business owners paying a lack of attention and under-investing in cyber resilience measures:

- They are barriers in and of themselves to investing in resilience measures.
- They shape the perceptions of small business owners about cyber threats.

While most small businesses are making some efforts to improve their cyber resilience, many are not able to implement the full range of resilience measures that would result in a step change in their resilience levels.

Our research shows that around 93 per cent of small businesses are taking at least one measure to protect their business from cyber risks.[61] However, the type of measures small businesses take vary significantly, with many using anti-virus software for example, but very few utilising Government schemes such as Cyber Essentials.

[60] Although it should be noted that even the smallest businesses are not completely identical to consumers. There are differences, which need to be acknowledged and recognised for policy making services. The point is that on a spectrum of characteristics, smaller businesses are closer to individual consumers in many of their behaviours and in terms of degree of market power than businesses that fall into the categories of larger-small, medium-sized and large. The implication of this insight is that for policy purposes a third category should be developed which recognises the similarities and differences between smaller businesses, consumers and larger-businesses.

[61] In response to FSB’s recent survey on crime against small businesses around three per cent said cyber resilience measures were not applicable to their business, a further three per cent said that they had not taken any measure and a half a percent of respondents did not know if they had taken measures. Consequently, around 93 per cent are taking at least one measure. Source: FSB, Business Crime Survey, 2016.

Table six: Small businesses and cyber resilience measures[62]
Source: FSB Business Crime Survey 2016

Resilience Measure	Proportion taking measure	Proportion of cyber crime victims taking the measure
Use computer security software	80%	86%
Backed up customer data and IT systems regularly	61%	66%
Performed regular updates of the software on your IT systems	53%	58%
Secured wireless network for the business	41%	45%
Store customer data offsite or on a separate device	27%	28%
Adopted a strict password policy	24%	26%
Trained staff in good IT security practices	20%	24%
Performed regular security risk assessments	11%	13%
Checked provider credentials and contracts when using 'cloud' and other online services	11%	11%
Blocked access to certain websites from work	9%	10%
Undertaken regular security testing	9%	10%
Encrypted all stored data	7%	7%
Background checked all employees	6%	6%
Taken out cyber-insurance	6%	6%
Encrypted communications	5%	5%
Sourced advice from the Government Cyber Streetwise and / or Get Safe Online	5%	6%
Have a written plan detailing measures to take, people and organisations to contact if attacked	4%	5%
Obtained a recognised security standard e.g. ISO 27001 or the Government's Cyber Essentials scheme	2%	2%
Sourced advice from the police	2%	2%

Encouragingly, 80 per cent of respondents had installed security software on their business IT. There is also a small but noticeable difference in take up of some security measures between victims and non-victims of cyber crime.

However, pattern is not replicated across all measures of security upgrades. This suggests that being a victim of cyber crime does not yet act as a driver of significant behaviour change. One implication of this is that other factors, such as 'social norms' in business may in fact drive behaviour more than the direct experience of being a victim of cyber crime. A Government looking to achieve a significant change would likely need to look at changing those 'social norms' among the small business community.

The fact that only around four in ten small businesses (41%) secured their wifi router and just over a quarter (27%), backed up business data either off-site or on a separate device and just under a quarter (24%) had a secure password policy, suggests that there is still some way to go to embed good cyber resilience practice among the small business community.

[62] FSB, Business Crime Survey, 2016.

Our research suggests that resilience might be increased if the vendors of many of the ICT products and services, which make up the digital infrastructure, made high security settings the default position.

The data also suggests that Government schemes and other independent security standards do not appear to be having much ‘cut-through’ with the small business community. Neither the Cyber Essentials Scheme nor ISO 27001 appear to have been adopted by the small businesses community n any significant scale.

While publicity and advice programmes such as Cyber Streetwise campaign and Get Safe Online are doing a bit better among small businesses (5%) they are yet to make the breakthrough into mass awareness among small businesses. This may, in part, be a reflection of the fragmentation of the advice and publicity. The latter is also reflected in the fact that a further two per cent of respondents were getting advice from the police. A single, uniform national message would likely improve the reach of cyber resilience advice to small businesses.

Small business owners often fail to accurately assess the risk posed by cyber crime

The low uptake of protection measures can in part be explained by the perceptions that small business owners have around cyber threats, which were catalogued by Cyber Streetwise in a survey carried out in 2015.

The Cyber Streetwise study found that:[63]

- Two thirds (66%) of small businesses were unaware of the risks of cyber crime or might be aware of it but do not consider it a risk.
- Over a fifth (22%) of respondents thought that small businesses aren’t a target for ‘hackers’ (22%).
- 26 per cent of respondents thought that only companies that take payments online are at risk of cyber crime.
- Just under a quarter thought that cyber security was too expensive.
- Just over a fifth (22%) confessed that they ‘…don’t know where to start’ when it comes to trying to deal with cyber threats.
- Only 16 per cent put improving their cyber security as a top priority for their business this year.

In contrast, larger businesses will often have access to dedicated staff who are better placed to determine the level of risk that cyber crime poses to their business, and to take appropriate action based on this assessment.

Organisational vulnerability: people, processes and procedures in small businesses

The constraints described above result in small businesses taking a very different approach towards processes and procedures compared to larger businesses. For those more able to afford it, the option of outsourcing IT issues to an external expert is often a route chosen. However, this approach does not internalise resilient processes and procedures and does not encourage staff to adopt optimal cyber resilient behaviours. Nevertheless, as recent research by Ipsos-Mori illustrates these two approaches are favoured by micro and small businesses:

[63] Cyber Streetwise, Is your business failing for any of the cyber security myths. Available at: https://www.cyberstreetwise.com/blog/your-business-falling-any-cyber-security-%E2%80%98myths%E2%80%99

> "Among micro firms, there was typically a more informal approach to cyber security and a relatively basic IT infrastructure, which meant that senior managers felt they could oversee cyber security themselves. Some small and medium firms employed an individual IT specialist but commented that, unlike large firms, they could not afford a whole team of specialist staff, and it was more cost-effective for them to outsource any maintenance that was beyond an individual staff member".[64]
>
> Klahr, R et al, Cyber Security Breaches Survey

The inevitable conclusion is that small businesses will remain vulnerable from the perspective of people, processes and procedures.[65]

High rewards and low risk for many cyber criminals: high rewards and low risk

Cyber criminals prey on both types of vulnerability outlined above. Those participating in cyber crime are highly organised, becoming increasingly sophisticated, driven by financial gain and often operate out of countries where law enforcement is challenging.[66] Large parts of the cyber criminals world operate like a parallel economy to the legitimate economy. There are criminal markets where cyber criminals can buy and sell cyber crime expertise and the data they have illegally obtained.[67]

The financial rewards are significant, while the risks for cyber criminals are low. Many of the methods used by cyber criminals, such as social engineering or vulnerability exploitation are cheap to deploy.[68] The risks associated with committing cyber crime are low because:

> "The perpetration of economic cyber crime outstrips preventative and other measures for control protection and has increased the difficulties of identifying, investigating and prosecuting offenders".[69]
>
> Levi, M et al, The Implications of Economic Cyber Crime for Policing

The difficulties faced by law enforcement agencies as a result of the challenges of technology have helped to make the online world a highly permissive environment for criminal activity. Academic Cameron Brown has outlined a long list of barriers that law enforcement and the criminal justice system face both domestically and internationally, if they are to effectively deal with cyber crime:[70]

- Identification – how the criminal and evidence can be identified when technology enables a large degree of anonymity and evidence being can be in large quantities of data.
- Access – it is becoming harder to access evidence because vital information may be stored remotely, it could be encrypted or it may require police forces from other countries to gather it.
- Liability – the complexity of rules around data protection and potential liabilities for private companies around data can impede the ability of businesses to co-operate.
- Policies and processes – where there are competing priorities cyber crime may not be able to be prioritised. In addition, it takes time to develop procedures which are commensurate with the challenges of technological change.
- Retrieval and retention – obtaining evidence from digital systems is difficult and time consuming and requires rules of evidence which recognise its difficulties. Similarly, it needs digital infrastructure providers to be co-operative, and respond speedily to requests for assistance.

[64] Klahr, R et al, Cyber Security Breaches Survey 2016: Main Report, 2016.

[65] Organisation vulnerabilities are not confined to smaller businesses. It should be noted that there are considerable issues with providers of key economic infrastructure which small businesses rely on. Problems with key infrastructure providers can have significant negative consequences for small businesses e.g. who need to pay a supplier or receive a payment from a customer: 'Standard best practice just does not happen. We meet CIOs and CTOs all the time and ask them what are the top-five business systems you need to protect and [keep] up and running. Many of them don't know what or who they're protecting or what they're protecting them from. If you don't even know what you're protecting in your business you don't know where to start or where to draw the battle lines,' Steer said'. Source: Coburn N et al, Cyber crime: The Fast Moving Menace, 2014. Available at: https://risk.thomsonreuters.com/sites/default/files/GRC01950.pdf

[66] Centre for Strategic and International Studies and McAfee, Net Losses; Estimating the Global Cost of Cybercrime, 2014.

[67] Centre for Strategic and International Studies and McAfee, Net Losses; Estimating the Global Cost of Cybercrime, 2014.

[68] Centre for Strategic and International Studies and McAfee, Net Losses; Estimating the Global Cost of Cybercrime, 2014.

[69] Levi, M et al, The Implications of Economic Cybercrime for Policing, 2015. Available at: https://www.cityoflondon.gov.uk/business/economic-research-and-information/research-publications/Documents/Research-2015/Economic-Cybercrime-FullReport.pdf

[70] Brown, C, Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice, International Journal of Cyber Criminology Vol 9 Issue 1, 2015.

- Admissibility and fairness – the complex nature of cyber investigations and evidence raises issues around the reliability of the evidence and whether the defence can effectively challenge evidence or conversely whether digital evidence might be too easily dismissed with the difficulties of obtaining it not recognised sufficiently.
- Human capital – investigators need to be sufficiently trained in cyber crime and technology issues. A lack of knowledge and capability risks undermining efforts against cyber crime.
- Technical resources and funding – law enforcement need specialist equipment to undertake effective investigations into cyber crime. Equipment is sophisticated and in order to ensure the tools remain adequate to the job, ongoing expenditure to keep it upgraded is likely to be required.
- Training – all those involved in the international law enforcement effort need to be continually trained so that they remain up-to-date with technological developments and cyber crime trends. If they are not they will not be effective.
- Underreporting and uncertainty – low levels of reporting of cyber crimes by the public do not help law enforcement build the accurate picture of cyber threats they need. During trials, uncertainty among judges or jurors about technical issues may result in failed prosecutions.
- Co-operation – formal regimes for co-operation may be too bureaucratic. Private sector organisations may fail to co-operate or at least be slow in co-operating.
- Legal framework and due process – laws that are not broad enough to encompass technological change can be a hindrance to prosecuting cyber criminals, while unclear rules on lead jurisdiction or procedures for resolving interjurisdictional conflicts may also act as a barrier.

THE WAY FORWARD

The cyber threat facing UK small businesses and the wider economy is significant and likely to continue to grow as more economic activity moves online. There is a clear risk that cyber crime will not only slow the growth of the digital economy but undermine its very foundations in the long-run, as the networks on which it is based become corrupted and trust breaks down.

FSB believes radical steps need to be taken individually, collectively, nationally and internationally if the risks to the economy posed by cyber threats are to be mitigated.

Mitigation has to begin with a comprehensive appraisal of the weaknesses in the digital economy and a more accurate understanding of the scale of the criminal activity.

Following this appraisal, a comprehensive approach to increasing cyber resilience across the economy is required.

The goal should be cyber resilience

The focus of Government and private sector policy and practices should be to increase resilience rather than simply cyber security.

Resilience is "the ability to adapt and respond rapidly to disruptions and maintain continuity of operations".[71] Applied to cyber threats this means networks and commercial supply chains need to have embedded within them "...the ability to continuously deliver the intended outcome despite adverse cyber events".[72]

Therefore, a focus on resilience should "...reduce the impact of... [cyber]... attacks and provide the ability to operate in the face of persistent attacks".[73]

Resilience provides the best opportunity to reduce the total cost of cyber threats. It is a result of a number of advantages as an objective over security alone. While security, and in particular prevention, are vital components of resilience, the concept also acknowledges the reality of:

- The desirability of some risk[74] as a result of the need for a degree of openness and exchange especially in digital technologies where change is occurring at a considerable pace.[75]
- The trade-offs that come with security i.e. efficacy of security measures on the one hand and operability (including network operability) on the other. Measures taken to reduce weaknesses - such as the erection of barriers to protect one element of the network from threats on the wider network - inevitably reduce the effectiveness of the network. If such a barrier is made too permeable then there is little point in it in the first place.
- The impracticality of protecting against, preventing and repelling all threats because, of their multiplicity and the speed at which they change.

Building resilience requires a shared approach

The question for policymakers, small and large businesses, individuals, developers and providers of the technological infrastructure is how to build resilience into the digital communication networks and commercial supply chains. Making these resilient will create a resilient economy best placed to reap the full benefits of the information technology revolution.

The scale of the losses to small businesses illustrate how current policy and private sector practice is failing to address the problem of cyber threats. A more resilient digital economy requires tackling the vulnerabilities outlined earlier. In order to do this, a collective effort by Government, business and individuals will be needed based on a long-term, ambitious, national strategy.

[71] Boyes, H, Resilience and Cyber Security of Technology in the Built Environment, 2013. Available at: https://www.cpni.gov.uk/documents/publications/2013/2013063-resilience_cyber_security_technology_built_environment.pdf?epslanguage=en-gb

[72] Bjork, F, Henkel, M, Stirna, S and Zdravkovic, J, Cyber Resilience – Fundamentals for a Definition, 2015.

[73] Symantec, The Cyber Resilience Blueprint: A New perspective on Security, 2014. Available at: https://www.symantec.com/content/en/us/enterprise/white_papers/b-cyber-resilience-blueprint-wp-0814.pdf

[74] 'Not only is eliminating risk impossible, but it impedes agility; an environment with an acceptable level of risk supports innovation'. Source: Symantec, The Cyber Resilience Blueprint: A New perspective on Security, 2014. Available at: http://www.symantec.com/en/uk/page.jsp?id=cyber-resilience

[75] Digital technologies are evolving rapidly. The Internet of Things will make connectivity ubiquitous, while more use of software as a service, platform as a service and infrastructure as a service create new risks. So too does the drive for ever more convenience and increasing consumerisation of technology. Source: Walder, B and Morales, C, Cyber Resilience: it's not about the 98 percent you catch, it's the 2 percent you miss. Available at: https://www.cisco.com/c/dam/r/en/uk/internet-of-everything-ioe/assets/pdfs/Cyber_Resilience.pdf

That combined effort will need to deliver, a number of significant long-term changes in the behaviour and practices of individuals, businesses and the Government.[76] Currently, technology is running ahead of the ability to adapt to the changes it is driving in personal and in particular economic activity. Practices in business and elsewhere remain largely 20th century and still best suited to the industrial age. They have not caught up with the digital economy.

Change however, needs to involve more than just 'catching-up' with current technology. It also needs to incorporate enough flexibility to enable further adaptation as the technologies now in use evolve or new ones emerge. Only by building in such flexibility can the UK economy become truly resilient in the very long-term.

UK Government progress to date

There is no doubt that the Government leads internationally on the cyber security agenda. From a standing start successive Governments have moved the UK forward significantly in the last decade in areas such as:

- The Government understands that an inclusive or shared approach is needed, which encourages all areas of society to invest in the objective of a more resilient economy. The Government has already made great strides towards this, for example, by working collaboratively with business to improve the cyber resilience of UK business.
- The UK Cyber Security Strategy in 2011 has helped focus and bring coherence to the cyber resilience policy agenda. The expected new five year strategy must be an ambitious one. It must not shy away from tough choices and outline, where appropriate, radical plans for further institutional reform and behaviour change.
- The Government has instigated some positive institutional reforms to ensure delivery of the current Cyber Security Strategy. This has included the creation of the Office of Cyber Security to co-ordinate cross-government activity on cyber resilience as part of a wider co-ordinated effort to improve resilience more generally.
- The Chancellor made a very encouraging speech in late 2015 laying out new policy ideas for improving the cyber resilience of the economy, including the creation of a one stop shop for cyber resilience information and advice for businesses.[77]

The National Cyber Security Centre (NCSC) is potentially a very positive step forward. As a single point of contact will allow small businesses to access the best information from a single trusted source.

Together, these measures provide the foundations for the next phase of reform to improve the UK's cyber resilience.

Next steps

While much of what the Government is doing is ambitious, there is still further to go to build a truly resilient small business sector and wider economy.

Small businesses should make a fair and sustained contribution to the overall cyber resilience of the UK economy but policy makers need to understand the constraints that exist for small businesses. Government policy needs to take a balanced approach by sharing the resilience burden proportionately among those best able to bear it.

Further improvements in the levels of cyber resilience among small businesses, commercial supply-chains and digital communications networks can only be achieved if a number of vital pre-requisites are put in place:

[76] Business will have to embed principle of resilience into its strategic planning and everyday activities as much as possible. The 'resilience cycle' has three elements: pre-disruption (sense and resist), disruption (react) and post-disruption (Adapt and re-shape). As EY state in their 2014 report on cyber-resilience: 'Organizations need to establish an understanding of the 'resilience cycle' helping...continuously build upon the experience of responding to threats'. Source: EY, Achieving resilience in the cyber eco-system, 2014.

[77] Osborne, G, Chancellor's speech to GCHQ on cyber security, 2015.

- The cyber resilience agenda needs to become one that all political parties prioritise and which all broadly agree on the direction of. The long term changes needed to improve the UK's cyber resilience can only be guaranteed if all political parties are invested in making them.
- Part of that long-term planning requires an ambitious National Cyber Resilience Strategy, building on the achievements of current UK Cyber Security Strategy. The expected new UK Cyber Security Strategy needs to be as radical as the scale of the risks.
- The principles and practices of cyber resilience need to permeate all of Government. This is even more imperative as the e-Government programme continues and more and more of the ways in which small businesses interact with the state move online. The Government has made considerable strides in establishing a strong cyber resilience co-ordinating function through the Office of Cyber Security and the National Resilience Team in the Cabinet Office.[78] But challenges remain, especially ones posed by technological development, such as:
    - The opportunities and risks that come from the use of big data.
    - The growth of the 'Internet of things'.[79]
    - The increasing sophistication of cyber criminals.
    - The digital skills gap in Government among Government employees and the similar gaps among the wider populace.
    - Increasing technological complexity as a result of growing interconnectedness through the ubiquity of internet enabled devices.

The Cabinet Office needs to ensure that Government becomes a practitioner of best cyber resilience practice, with in-built flexibility for continuous adaption as the state of technology requires.[80]

[78] DGSF, The Future of Information Security: Executive Summary and Conclusions, 2015. Available at: https://www.digitalgovernmentsecurityforum.org/?wpfb_dl=27

[79] The 'Internet of things' is the umbrella term for the extension of digital connectivity i.e. the ability to collect and exchange information to a wide range of objects and devices beyond the traditional computer and mobile phone.

[80] College of St George, in partnership with DCLG, iNetwork, City of London Corporation and the BCS identified the need for a more collaborative approach between national and local government to improve the cyber-resilience of Government. Source: College of St George, Local leadership in a Cyber Society: Towards a model for Civic Cyber Resilience, 2016.
Available at: https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Local%20Leadership%20in%20Cyber%20Society%20Report.pdf

THE POLICY RESPONSE

The problems which keep both resilience levels low across the small business community and the risks from cyber threats high are numerous and interdependent. The indivisibility of the various vulnerabilities mean that tackling just one of them will fail to deliver much overall improvement in the cyber risk landscape. The problems need to be tackled holistically and systematically. Therefore, the policy response required is a multi-faceted one operating on many fronts at the same time.

Underpinning specific policy measures should be an understanding that the approach has to be a shared one. Public and private sectors each need to take their share of the responsibility. The Government have made this understanding a key part of their strategy so far. However, the sharing of the burden of responsibility needs to be somewhat re-balanced if the shared approach is to deliver the objective of a more cyber resilient small business sector and economy.

The current sharing of the burden places too much of it on the small businesses who are least well positioned to effectively deal with cyber risks. The current distribution does not place enough responsibility on other groups who have access to more resources to most effectively tackle the vulnerabilities of digital information networks and the supply-chains of the economy.

The policy response required to achieve the type of re-balancing needed across the public and private sectors, can be divided up into areas for action by Government and the private sector. Further, specific measures can be split into those aimed at tackling each of the causes of the increasing cyber risk faced by small businesses and the economy. Specifically:

- Minimising organisational vulnerabilities requires measures that will encourage a permanent shift in UK business culture and practice towards more cyber awareness and greater knowledge and sophistication among the small businesses population about how to be cyber resilient. People, processes and procedures may then be able to catch up with the technological changes that have taken place over the last 25 years and which continue to take place.
- Reducing technological vulnerabilities will require measures that encourage those best placed to deal with the vulnerabilities to do so. Relying on those least able to organise and implement the best measures will not deliver the improved resilience needed. This will require something of a shift in the existing security paradigm.
- Reducing cyber criminal’s opportunities to operate successfully can only be achieved by increasing the risks for cyber criminals of perpetrating cyber crimes through more effective disruption, investigation and prosecution.

These measures can be categorised into ones that can be implemented fairly swiftly i.e. in the short to medium-term and those that will take much longer to implement.

Sharing responsibility for cyber resilience

The role of Government in increasing cyber resilience

Government has a key role to play through establishing the framework within which all parties operate. Getting this wrong can cause significant problems and unanticipated consequences in the long term. Not all risks can be anticipated however. This is particularly the case when regulating complex systems like digital communications networks, supply chains and economies.

While the case for an expanded role for the Government in relation to cyber resilience is a strong one - it has to be a carefully expanded role in order to minimise negative impacts on complex systems.

Expanded responsibility of Government should include:

- Reforming their approach to regulation ensuring the resilience of Government services to the private sector.
- Creating a regulatory environment which incentivises better security behaviour across the private sector, especially by those with the resources and expertise to deliver the best outcomes.
- The provision of greater levels of bespoke support and the right incentives for small businesses to increase their cyber resilience.
- More long term investment in building deterrent capability e.g. the capacity of law enforcement.

The role of the private sector in increasing cyber resilience

The private sector also needs to adapt to improve overall cyber resilience. The rebalancing of responsibility within the private sector should include:

- Businesses taking as much responsibility as is practical for them to do so. Small businesses need to be made more aware of the risks that come through operating online. Only with a better understanding of the risks and the possible negative impact they can have, will small businesses be able to adjust their practices and processes in the most effective ways. Owing to the constraints they operate under, small businesses need support from others to help take the actions necessary to increase their cyber resilience. There are also many things that resource and knowledge constraints mean small businesses will not be able to do or are not best placed to do.
- More measures taken by the digital infrastructure providers to help protect users who are not adequately resourced to protect themselves, such as small businesses.
- The larger economic infrastructure providers taking more responsibility through increasing the cyber resilience of their systems and practices, in addition to helping their vulnerable users, such as small businesses, improve their own cyber resilience.

1. Strong foundations for cyber resilience policy

Before outlining specific measures aimed at dealing with the three categories of causes of cyber risk, Government can make a number of reforms that will provide a set of strong foundations.

A more flexible approach to regulation

Before looking at specific areas of regulation or specific regulations and regulatory reforms, the Government should look in detail at:

- Its general approach to regulating cyber resilience issues. The fast changing world of cyber threats and the risks they pose raise questions about the viability of aspects of the current mode of regulation.
- Making sure that its ability to deliver services to the business community is resilient. There is little point in the Government playing a major role in implementing measures to help and encourage the private sector to be more cyber resilient if Government is not sufficiently resilient itself.

Regulating for cyber resilience

Traditional regulation is based on a prescriptive command and control model, where detailed standards are set out and compliance with those standards is monitored through reporting and external inspection.

These standards do not usually reflect risk, but instead are based on hazard. The latter can lead to regulatory micro-management and unnecessary burdens rather than generating buy in from those being regulated. This hinders the development of broader behavioural changes which are needed to change the norms of complex systems.

The problems of regulating security issues associated with the digital communications technologies this way, are well known:

> “Regulations that dictate specific solutions can be a poor fit for cyberspace…[a]…focus on compliance can turn security from an iterative, adaptive process to an organisational routine disconnected from the risks faced. Compliance replaces accountability, since organisations can avoid any decision that might improve security”.[81]
>
> Singer, P W and Friedman A, Cyber Security and Cyber War: what everyone needs to know

[81] Singer, P W and Friedman A, Cyber Security and Cyber War: what everyone needs to know, 2014.

The shift in recent years in some policy areas towards a more principles based approach to regulation has not resulted in a radical improvement in either regulatory outcomes or reductions in regulatory burdens.

The principles based approach is often still largely based on either reporting and/or external inspection. However, it does have benefits that the more prescriptive approach tends to lack, as its flexibility helps facilitate innovation. However, the downside is greater uncertainty (compared to the prescriptive approach) about past and future regulatory risks which can lead to potentially 'chilling' effects on business activity.

A middle way is needed between these two modes of regulation when seeking to develop greater cyber resilience. Where dynamic complex systems with opportunities for unintended consequences from regulatory interventions exist, it is vital that regulatory systems themselves adopt some of the most successful aspects of complex systems.

Regulating to improve cyber resilience therefore requires a framework which will encourage an iterative and adaptive process that encourages innovation and entrepreneurship. The Government is likely to get the best regulatory results from a system which:

- Incentivises beneficial behaviours and norms (through transparency, accountability and pro-activity) among the regulated which benefit the whole system e.g. information sharing.
- Recognises that systems are complex. Prescriptive one size fits all regulatory solutions are unlikely to work satisfactorily.
- Encourages the spread and adoption of the most effective resilience solutions by all as well as the development of new and better solutions.
- Is flexible and has learning and adaptation built into it.[82] Institutionalised learning and adaptation are often absent from both traditional prescriptive and principles-based regulatory modalities.

Short / medium-term policy recommendations to improve regulatory outcomes

As part of its review into the regulatory framework around cyber security, the Government should undertake a fundamental look at its methods of regulation as well as what types of regulations are needed and where. It should review the current approach to regulation against the principles outlined above, to decide what the best general approach for the future might be.

2. Resilient Government services

More and more of the interactions that small businesses have with Government are moving online, as the Government pursues a digital by default agenda. Government, in addition to its regulatory role, is a key player in digital information networks.

It is crucial that Government systems are resilient in the face of cyber attacks. Strategies need to be in place that not just prevent cyber criminals and foreign Governments from attacking Government assets and services, but also ensure that, should attacks succeed, Government services can recover and continue with as little disruption as possible.

The digital by default agenda must not forget resilience. The Government has this on its agenda, with the Cabinet Office leading efforts to ensure that Government services are resilient in the face of the growing threat from cyber crime. This needs to continue to be the case.

[82] Murray, A D, The Regulation of Cyberspace: Control in the Online Environment, 2007.

Lessons from the experience of other countries should also be taken on board. Countries, such as Singapore, Denmark and Estonia are leading in e-Government best practice.[83] Part of e-Government should be embracing and embedding the principles that are being developed in the private sector into policy and administrative reform activities, such as:

- Real-time information sharing.
- Feedback and learning from users and other service providers.
- Flexibility and adaptation in light of that learning.
- Resilience built into systems with robust resilience planning, procedures and processes.[84]

Short / medium-term policy recommendations to deliver resilient Government services

The Government should continue to engage with international partners to exchange information and best practice on the adoption of e-Government. The Government should ensure that the primary focus of such international discussions is on ensuring that high levels of cyber resilience are built into Government services. A formal international benchmarking system should be introduced to spread best practice.

This will require engaging fully with:

- Organisation for Economic Co-operation and Development (OECD) initiatives in the area of e-Government and pushing for the development of detailed comparative work on the cyber resilience aspects of e-Government.
- The United Nation's Division for Public Administration and Development Management (DPADM) and their work to promote e-Government internationally.
- Other Governments and leveraging in their expertise directly to the UK's programme where possible.

Long-term policy recommendations to deliver resilient Government services

Government must retain an offline option for all main Government services that small businesses use. Maintaining an offline capability is the only guarantee of a resilient Government and the continuation of key services during and in the aftermath of cybe attacks.

3. Dealing with organisational vulnerabilities: changing business culture and practice

User vulnerability needs to be reduced. The most effective way to generate a step change in this category of vulnerability is to change business culture and practice across the small business sector. Cyber resilience and associated procedures and processes should become a key part of day to day business activity, a central feature of business planning and seen as being as important as finding new customers, obtaining finance and paying taxes in the minds of small business owners and managers.[85]

[83] The Waseda University and IAC International E-Government Rankings Survey identified Singapore as the leading practitioner of e-Government, ranking top in Management Optimization and GCIO. While Denmark ranks top for online services, National Portal and Cyber Security. Estonia ranks second in Online Services, E-Participation, National Portal and Cyber Security. Source: Obi, T ed, 2015 – Waseda – IAC International E-Government Ranking Survey, 2015.

[84] As EY state in their 2014 report on cyber-resilience: 'Organizations need to establish an understanding of the 'resilience cycle' helping...continuously build upon the experience of responding to threats'. The 'resilience cycle' which offers a framework for ensuring resilience within organisations and systems has three elements: pre-disruption (sense and resist), disruption (react) and post-disruption (Adapt and re-shape). Source: EY, Achieving resilience in the cyber eco-system, 2014.

[85] Symantec, The Cyber Resilience Blueprint: A New perspective on Security, 2014.
Available at: http://www.symantec.com/content/en/us/enterprise/white_papers/b-cyber-resilience-blueprint-wp-0814.pdf

This can only be achieved through:

- Raising the awareness levels of small business owners about the existence of cyber risks in the first instance and then the scale and types of risks to their business interests.
- Giving them the tools (including the knowledge) to improve the cyber resilience of their business.
- Encouraging them to fully integrate cyber resilience into their business activity through incentives and other behaviour changing mechanisms.

Government can therefore play a significant role in helping improve the situation across all three of these areas.

Short / medium-term policy recommendations for Government to change business culture

Consolidate the existing awareness raising campaigns around cyber security into one coherent set of messages along with a nation wide campaign. This should build on the success of the Cyber Streetwise and Get Safe Online campaigns with a bespoke element targeted at small businesses. The ambition for the campaign should be similar to a long-term public health campaign aimed at nationwide behaviour change among businesses.

Give the National Cyber Security Centre responsibility for the national awareness raising campaign.

Ensure that the small business voice informs the information provision and advice offered by the National Cyber Security Centre. The tailored messaging needed when communicating with small businesses requires an understanding of the unique characteristics of small businesses. Small business groups, with their expertise in reaching out to the small business community, should have a role in sign posting and the dissemination of the key messages.

The Innovation Vouchers scheme for cyber security should be significantly expanded. Every business in the UK should be entitled to a voucher. The ways in they can be used should be increased to include not just the purchase of consultancy but the purchase of new secure hardware and cyber security systems.

Longer term policy recommendations for Government to change business culture

Ensure the National Cyber Security Centre has sufficient resources to raise its profile. The profile of the National Cyber Security Centre needs to be raised to that of other well-known national institutions. Almost everyone, especially business, in the UK should know that the National Cyber Security Centre is the place to go for basic trusted advice about cyber resilience.

The National Cyber Security Centre should run the Government's Cyber Essentials Scheme.

The Cyber Essentials Scheme should be expanded. It should have a focus on the wider concept of resilience rather than just security. As part of this expansion, the scheme should help small businesses to think and operate more strategically in relation to cyber resilience. The scheme should include the provision of template resilience packages, for small businesses.

Encourage larger businesses to support the small businesses in their supply chains to adopt effective cyber resilience practices. The Government should consult on whether benefits might accrue from:

- Enabling small businesses to use their Innovation Vouchers to purchase cyber security advice and support from a larger customer company.
- An expansion of the Cyber Essentials Scheme for larger companies that help their small suppliers adopt good cyber practices.
- Use of the tax system to incentivise larger companies to take an interest in the cyber resilience of their small suppliers.

Boost the use of cyber insurance among small businesses by supporting the development of an effective market in quality small business cyber insurance products. One way of boosting the use of cyber insurance is through encouraging initiatives which aim to establish consistent credible industry standards for such products.

Cyber insurance can play a useful role in helping small businesses survive and thrive again after a cyber attack. It can also create incentives to incorporate good cyber practices by requiring certain minimum standards of security behaviour from those being insured.[86]

The market is currently underdeveloped. There is considerable variation in the quality and cost of products available. A concerted effort needs to be made to establish minimum insurance quality standards for cyber insurance which should help make cyber insurance more affordable. In addition, there needs to be help for small businesses to navigate the nascent market to ensure they can get the right policy.

If the market fails to deliver, on any significant scale, the types of cyber insurance products small businesses need, then the Government should consider the merits of further interventions. This could include developing a similar initiative to the Flood Re initiative for cyber resilience insurance.

Government should consider making cyber insurance compulsory for businesses above a certain size or in high-risk sectors. This should be an option contingent on a sufficiently effective cyber insurance market developing.

While a radical step, insurance can incentivise the implementation of best practice among those subject to insurance requirements. Therefore, for high-risk businesses or those over a certain size the costs of insurance are more proportionate to the problem. In such circumstances a policy of compulsion becomes more justifiable on the grounds that the benefits to both individual businesses and the wider economic system outweigh the costs.

Encourage small business owners to improve their digital skills. The level of digital skills among the small business community mirror those of the wider UK population. The digital skills of the latter have been well documented and it is clear that there is room for improvement.[87] In addition to addressing the digital skills gap in order to exploit the challenges of the digital age, small businesses require educating on the importance of cyber security and the available tools to protect themselves against threat. Improvement in digital skills will help embed better cyber resilient behaviours and policies in small businesses. The Government should:

- Use the National Cyber Security Centre as a sign posting hub for small businesses to existing cyber security and resilience training. This, along with the development of a National Cyber Security Centre accreditation scheme, should help smaller firms navigate the market and know whether they can expect a minimum level of quality.
- Incorporate (accredited) training courses into the requirements for the more advanced levels of the expanded Cyber Essentials Scheme.
- Allow small businesses to use part of their Innovation Vouchers to purchase relevant training (and top-up the vouchers with their own funds where necessary) for owners, managers or employees.
- The existing Academic Centres of Excellence in Cyber Security Research and their associated higher educational institutions should be encouraged to develop training courses aimed at up-skilling the small business community in their areas, in cyber resilience skills. The Government should provide some seed funding to encourage this development.

Teach cyber resilience in schools alongside the other aspects of ICT already being taught. Basic digital skills, including how to stay safe and secure online, should be embedded in the curriculum as a core part of the functional skills that every young person should acquire during their education. This should begin in primary school and continue until the end of compulsory

[86] As noted by Singer and Friedman: 'Former national counter-intelligence executive Joel Brenner explains, 'Insurers play an important role in raising standards because they tie premiums to good practices…'. Source: Singer, P W and Friedman A, Cyber Security and Cyber War: what everyone needs to know, 2014.

[87] The UK is currently experiencing a digital skills gap. It is estimated that approximately 23 per cent of the UK population lack at least one basic digital skill. Source: In addition to addressing the digital skills gap in order to exploit the challenges of the digital age, small businesses require educating on the importance of cyber security and the tools to protect themselves against threat. Source: Centre for Economics and Business Research, The economic impact of basic digital skills and inclusion in the UK: A report for Tinder Foundation and Go ON UK, 2015.

education.[88] In their recent report to the Government, the House of Lords Digital Skills Committee said that teaching of digital skills in schools should be regarded as equally important as lessons in numeracy and literacy if the UK is to successfully pursue a digital agenda.[89]

As the Government has promised, the **Cyber Information Sharing Partnership (CISP) should be brought within the remit of the National Cyber Security Centre at the earliest possible moment.**

Expand the CISP with compulsory participation for all large and medium-sized businesses and explore the possibility over the long term of bringing in more of the small business population too.

The provision of better information to businesses about current cyber threats through an expanded CISP is important.[90] For the private sector access to the latest threat information is vital if businesses are to improve their resilience efforts swiftly enough to protect themselves.[91]

Similarly, law enforcement authorities need to know what risks business currently face so that they can take appropriate action too. This can only be achieved if as much of the UK business population, as is reasonable, are invested in information sharing. With compulsory participation, a further option to ensure a proportionate burden could be to enable degrees of participation, so that low risk businesses do not have to be as 'participative' as higher-risk businesses.

4. Minimising technological vulnerabilities: building security into the infrastructure

Protection against cyber attacks through technological measures is one of the main ways that cyber crime in particular, and cyber risks more generally, will be significantly reduced. A report for the City of London Police suggested that it should be the primary way that cyber crime is dealt with.[92]

However, the current approach to prevention relies upon those least able to deliver the most effective outcomes to bear the heaviest burden. This has been recognised by leading scholars such as Professor Ross Anderson[93] and senior policymakers on the House of Lords Science and Technology Committee.[94] A better balance is needed than the one that exists at the moment .

The Government is beginning to recognise the problems with this approach. The Chancellor outlined in his speech to GCHQ that ISPs might be able to play a role in reducing the cyber risks faced by vulnerable users of the internet, such as small businesses. However, in order to deliver a long-term step change in cyber resilience, the Government needs to go further and encourage digital infrastructure providers to bear more of the resilience burden. In order to achieve this there are a series of measures the Government should take.

Short-term policy recommendations to minimise technology vulnerabilities

Require software providers, especially those providing cyber security software, to make automatic patching and updates the default option on all products. Hardware suppliers, such as providers of wifi routers, should also have to have adequate security features bundled in with their products and for the default setting to the highest strength possible when active.

[88] Such a change would complement recent changes the Government has made to the national curriculum which have seen ICT (Information and Communications Technology) being replaced by a new 'computing' curriculum, including coding lessons for children as young as five. In addition, helping young people understand the importance of cyber security and staying safe online should form a key part of the teaching of wider life skills in order to prepare them to take their next steps after formal education, both personally and into the labour market.

[89] House of Lords Select Committee on Digital Skills, Make or Break: The UK's Digital Future, 2015.

[90] It is encouraging that the Government sees this as important too and that progress has already been made in this area. Source: Osborne, G, Chancellor's speech to GCHQ on cyber security, 2015. Available at: https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security

[91] FSB has long called for more partnership working and information sharing within the private sector about cyber-risks and best cyber-resilience practice. Source: FSB Cyber security and fraud: The impact on small businesses, 2013.

[92] The prevention approach has been the one advocated recently in a report for the City of London Police as the primary way to deal with the cyber crime issue. The report is fairly fatalistic about the ability of the police to investigate, arrest and prosecute cyber-criminals in sufficient enough numbers. Source: Levi, M et al, The Implications of Economic Cybercrime for Policing, 2015.
Available at: https://www.cityoflondon.gov.uk/business/economic-research-and-information/research-publications/Documents/Research-2015/Economic-Cybercrime-FullReport.pdf

[93] Anderson, R, Why Information Security is Hard – An Economic Perspective. Available at: https://www.acsac.org/2001/papers/110.pdf

[94] House of Lords Science and Technology Committee, Personal Internet Security', 2007. Available at: https://books.google.co.uk/books?id=W--x_sFoMK8C&pg=PA238&lpg=PA238&dq=House+Of+Lords+Science+and+Technology+Committee+end+user+cyber&source=bl&ots=AR3vO049zG&sig=sltO4AJDPcwfGSYHc-m0GeKu-gq4&hl=en&sa=X&ved=0ahUKEwiZ-cv-kpXKAhVLXRQKHbZ5DiAQ6AEIPjAG#v=onepage&q=House%20Of%20Lords%20Science%20and%20Technology%20Committee%20end%20user%20cyber&f=false
van Eeten and Bauer describe how the incentives faced by individuals and organisations are mis-aligned. The result of this mis-alignment is that detrimental behaviour and vulnerabilities are encouraged because the full costs of negligent behaviour are not, in large part, borne by those who generate those costs through their activities. Source: van Eeten, M. J. G and Bauer, J, The Economics of Malware: security decisions, incentives and externalities, 2008.
Available at: http://www.oecd.org/internet/ieconomy/40722462.pdf

Longer term policy recommendations to minimise technology vulnerabilities

Reform the legal framework governing vendor liability to create better incentives to incorporate adequate security into products and services.

A key driver of the vulnerability of much of the infrastructure of the digital economy results from a misaligned incentives for those who build and maintain the infrastructure. There is an important role for setting the right incentive structure. Many of the recommendations by the House of Lords Science and Technology Committee from 2006-7 still hold true today. The Government should:

- Make proposals for a regime of proportionate product liability on software and hardware vendors.
- Based on evidence from the liability changes, be prepared to develop and implement a comprehensive liability regime.[95]

As part of the evolution of vendor liability, web developers and administrators need to be brought within a liability regime. Many insecurities and successful 'hacks' are the result of insecure web programming.

Symantec have identified that there are:

> "Major security vulnerabilities in three quarters of popular websites...There were over one million web attacks against people each and every day in 2015. Many people believe that keeping to well-known, legitimate websites will keep them safe from online crime. This is not true. Cyber criminals continue to take advantage of vulnerabilities in legitimate websites to infect users, because website administrators fail to secure their websites. More than 75 percent of all legitimate websites have unpatched vulnerabilities. Fifteen percent of legitimate websites have vulnerabilities deemed 'critical,' which means it takes trivial effort for cyber criminals to gain access and manipulate these sites for their own purposes. It's time for website administrators to step up and address the risks more aggressively".[96]
>
> Symantec, Internet Security Threat Report: Volume 21

The Government should press ahead with encouraging ISPs to take a leading role in tackling cyber threats.

As the Chancellor stated in his speech to GCHQ in 2015:

> "We will explore whether they can work together – with our help – to provide this protection on a national level.
>
> We cannot create a hermetic seal around the country – indeed it wouldn't be in our interests to have one – but with the right systems and tools our private internet service providers could kick out a high proportion of the malware in the UK internet, and block the addresses which we know are doing nothing but scamming, tricking and attacking British internet users" .[97]
>
> Osborne, G, Chancellor's speech to GCHQ on cyber security

This is a welcome step. There is evidence to suggest that filtering of malware can be quite effective without imposing excessive costs.[98] Encouraging ISPs to take a more prominent role in this way would add in an extra layer of protection to digital infrastructure and for vulnerable users like small

[95] House of Lords Science and Technology Committee, Personal Internet Security: 5th Report of Session 2006-7', 2007. Available at: http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/165i.pdf One option for such a comprehensive regime might include a 'lemon law' whereby software, website design and other products and services, which fail beyond a certain level have to give refunds to users. Another is a regime very similar to that which prevails in relation to many physical products i.e. a strict liability safety regime. There are a number of options that might be followed and should be explored in the long-term.

[96] Symantec, Internet Security Threat Report: Volume 21, 2016.

[97] Osborne, G, Chancellor's speech to GCHQ on cyber security, 2015. Available at: https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security

[98] Andelin, P, ISP Level Malware Filtering: An Extended Clean Feed? Available at: http://www.lavasoft.com/support/spywareeducationcenter/wp_ispmalwarefiltering.php

businesses.[99] Ideally, security should be an issue on which ISPs compete.[100] Relevant regulators should work to establish a system to help small business customers understand the level of security different providers' offer and make the most appropriate purchasing decisions. However, **to ensure action is taken, the Government should legislate for a 'back-stop' legal requirement for ISPs to undertake activities such as malware filtering across their networks and improve their general approach to security,** should a voluntary approach prove inadequate.

A 'back-stop' power would need sufficient penalties to ensure incentives to operate such a system were robust. The Government should look at whether the best of way of creating such a framework is to remove the ISP's mere conduit protections, as recommended by the House of Lords Science and Technology Committee. A sensible qualification to blanket liability might be a time-limited 'immunity' to encourage ISPs to be proactive in their monitoring and filtering.

Another measure the Government should consider as part of the 'back-stop' power package is a requirement for ISPs to restrict access to the internet if a user was infected with a worm and was contributing to the continued infection of the network.

In addition to sharing the burden of resilience among digital infrastructure providers, the burden should be further shared among the larger providers of economic infrastructure such as banks. Businesses in these sectors play just as an essential role in enabling economic activity as the providers of the digital infrastructure.

Similarly, users of such services such as small businesses, tend to bear much of the burden of the vulnerabilities in the systems which deliver the economic infrastructure services. This ranges from having to suffer the cost of unknowingly processing a fraudulent card transaction to not having any guarantee that monies stolen from a small business's bank account e.g. by 'hackers' will be refunded to the business. Yet they are often the least able to bear the resilience burden.

As long as banks and other financial intermediaries can remain exempt from any formal responsibility to ensure that users and their systems are as secure as possible, there is no incentive for them to deliver significant security improvements. Yet it is the banks that have the resources to best understand the range of cyber threats and the areas of risk and to invest to reduce them.

Larger economic infrastructure providers such as financial intermediaries should be liable for losses as a result of cyber crimes such as online theft and fraud.

Financial intermediaries have the resources to be much more proactive in dealing with cyber crime and invest in the best technology to tackle e-fraud and other online financial crimes compared to small businesses. As the House of Lords Science and Technology Committee highlighted - albeit in relation to consumers - placing liability on the bank for online fraud would be consistent with existing principles in the common law and in the Bills of Exchange Act 1882, which sets out this principle with regard to cheques.

5. Tackling cyber criminals through concerted law enforcement action

The vulnerability of the networks and supply chains that form the modern economy can be further reduced through more effectively dealing with those who undertake cyber criminal activity.

[99] As Rowe et al highlight in their Research Briefing '...studies and security experts have suggested that Internet Service Providers (ISPs) may be in a good position to cost-effectively prevent certain types of malicious cyber behaviour...are ideally suited to mitigate a variety of cyber security issues...ISPs observe traffic flowing into and out of their networks. They are in a position to observe traffic spikes that could be associated with excessive malicious traffic (e.g., caused by worms or spam bots) and 'filter' suspicious traffic. For example, ISPs could stop suspicious traffic from entering their network...'. Source: Rowe, B et al, The Role of Internet Service Providers in Cyber Security, 2011.

[100] As Pekka Andelin notes: 'Providing malware filtering as an extension of the existing clean feed could prove to be a competitive advantage for ISPs that offer such solutions to their customers'. Source: Andelin, P, ISP Level Malware Filtering: An Extended Clean Feed?
Available at: http://www.lavasoft.com/support/spywareeducationcenter/wp_ispmalwarefiltering.php

The difficulties of law enforcement in the digital age

Law enforcement is much more difficult in the information age.[101] As the Police Foundation have observed:

> "Technological changes, with concomitant changes in patterns of crime and demands for security…present enormous operational challenges for the police service in working across borders (both local/regional and national) and in keeping up to speed with rapid changes in the modus operandi of criminals and their associates. Responding effectively to these developments while attempting to meet increasing public and political demands for security, and adapting to the prospect of long-term budgetary restraint and wider police reform, present some significant challenges for the service".[102]
>
> Karn, J, Policing and Crime Reduction: the evidence and its implications

Evidence suggests that the UK's cyber policing capabilities are not yet at the levels required to effectively tackle the growing threat of cyber crime. While the police are making progress a number of HMIC reports have found that there is still some way to go before local and regional policing in the UK can meet the 'Strategic Policing Requirement' on cyber crime.[103] Part of that shortfall manifests itself in an often inadequate response by the police forces in England and Wales to victims of i.e. cyber crimes.[104]

While the arrests and prosecutions of cyber criminals is largely carried out at a local level, investigations are often global and multi-jurisdictional.[105] This requires a globally networked policing and judicial effort on a very significant scale combined with a level of police, judicial and private sector co-operation that, similarly, has never previously been the case. Yet, there are considerable hurdles to effective international law enforcement co-operation too.[106]

What can be done?

With adequate will and investment there is much that can be done. As CSIS and McAfee have emphasised, effective action is '…well within the realm of the possible if people decide to treat cybercrime seriously and take action against it'.[107]

There is mounting evidence that 'Law enforcement has become more effective at catching cyber criminals…and high-profile successes at disrupting them…[illustrate]…how coordinated, international efforts can pay dividends'.[108] For example, '…police shut down several major financial botnets in 2014'.[109] Specific recent examples of this growing effectiveness include:

- The shutting down of the group controlling the Dyre financial fraud Trojan.[110]
- Police in 19 countries arrested over 90 people involved in developing and perpetuating 'creepware' spyware.[111]

[101] Shinder, D, What makes cybercrime laws so difficult to enforce, 2011. Available at: http://www.techrepublic.com/blog/it-security/what-makes-cybercrime-laws-so-difficult-to-enforce/

[102] Karn, J, Policing and Crime Reduction: the evidence and its implications, 2013. Available at: http://www.police-foundation.org.uk/uploads/holding/projects/policing_and_crime_reduction.pdf

[103] HMIC, The Strategic Policing Requirement: An inspection of how police forces in England and Wales deal with threats of a large scale cyber incident, 2014. Available at: https://www.justiceinspectorates.gov.uk/hmic/wp-content/uploads/strategic-policing-requirement-cyber crime-2014-06.pdf (Home Office, The Strategic Policing Requirement, 2015. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/417116/The_Strategic_Policing_Requirement.pdf)

[104] HMIC, Real lives, real crimes: A study of digital crime and policing, 2015. Available at: https://www.justiceinspectorates.gov.uk/hmic/our-work/digital-crime-and-policing/real-lives-real-crimes-a-study-of-digital-crime-and-policing/

[105] As Symantec note: 'Rarely is an attack group confined to one country, and with major groups spanning multiple jurisdictions, cross-border cooperation with law enforcement is an important factor to ensure that these successes continue to strike a blow against cybercriminals'. Source: Symantec, Internet Security Threat Report: Volume 21, 2016.

[106] As the academic David S Wall has observed: 'The second challenge is the problem of….legal disparities in inter-jurisdictional cases. Protocols…rely on upon the offence in question being given similar priority in each jurisdiction If…a criminal offence carries a strong mandate from the public…then resourcing its investigation is usually fairly unproblematic…However, where there is not such…[a]…mandate then resourcing becomes problematic…the other inter-jurisdictional problem is… cultural differences in defining the seriousness of specific forms of offending, or some offences may fall under civil law in one jurisdiction and criminal law in another, as is the case in the theft of trade secrets…'. Source: Wall, D E, Cybercrime, 2007.

[107] Centre for Strategic and International Studies, Net Losses; Estimating the Global Cost of Cybercrime, 2014.

[108] Symantec, Internet Security Threat Report: Volume 21, 2016.

[109] Symantec, Internet Security Threat Report: Volume 21, 2016.

[110] Symantec, Internet Security Threat Report: Volume 21, 2016.

[111] Symantec, Internet Security Threat Report 20, 2015.

- This seizure, by law enforcement, of vital infrastructure (such as command and control servers) used by Simda botnet's controllers.[112]

Domestically, the efforts' made to improve the law enforcement response to cyber crime have manifested themselves most visibly through a number of organisational changes:[113]

- The National Crime Agency (NCA) contains the National Cyber Crime Unit (NCCU), which leads the national response to organised cyber crime.
- At the regional level Regional Organised Crime Units (ROCUs) have been established. They have a number of roles. ROCUs support local cyber crime focused law enforcement activity through providing a single point of contact, expertise and specialist tools to local forces, investigate the most serious cyber crimes in their regions, support the NCCU where appropriate and co-ordinate cross-boundary investigations.
- The National Police Chief's Council, the College of Policing and Home Office have established the Digital Investigation and Intelligence (DII) Management Group to co-ordinate the build-up of digital capabilities across all police forces and ensure minimum standards of capability and competence. At the same time the College of Policing has developed a framework on regional capability which can be used to assess the performance of regional forces in establishing their capabilities for tackling cyber crime. In addition, the College have developed numerous e-learning packages for all police officers to improve their cyber skill levels.

However, gaps in capacity and capability remain at the local and regional levels in particular. At the local level, HMIC have suggested how the police service could improve its response and better tackle the increasing problem of cyber crime. The police need to:[114]

- Urgently develop a better understanding of the scale and impact of cyber crime at all levels.
- Devise and implement more effective ways of responding to it through putting in place the right leadership and governance arrangements and strategies at all levels to deal with cyber crime appropriately.
- Utilise private sector expertise and develop the skills of those already in the police force. This should help ensure every force has the capability and capacity to respond to cyber crime in an equally effective way as other crime.

At the regional level, HMIC noted that the ROCU's could be further strengthened to improve the regional coordinated response to cyber crime. The capacity for dealing with cyber crime was considered inadequate by HMIC with seven of the ROCUs having less than 10 staff working on cyber crime.[115] Further, cyber crime tended to be treated as a category of criminal activity separate to other criminal activities such as organised crime, when in fact it is highly integrated with organised crime.[116]

As a result of the immature stage of development that cyber policing capabilities are at, HMIC have made a raft of suggested improvements in operational capability, consistency and co-ordination to build on what has already been achieved by ROCUs:[117]

- Better integrate the effort against cyber crime with the wider activity against organised crime.
- The ROCUs need to be better integrated with the NCA.
- The prioritisation of the delivery of '...an integrated approach to sharing and using intelligence'.[118]

[112] Symantec, Internet Security Threat Report: Volume 21, 2016.

[113] techUK, Partners against crime: How can industry help the police fight cyber crime, 2015.
Available at: https://www.techuk.org/insights/reports/item/6102-techuk-calls-on-police-and-industry-to-work-together-to-tackle-cyber crime

[114] HMIC, Real lives, real crimes: A study of digital crime and policing, 2015.
Available at: https://www.justiceinspectorates.gov.uk/hmic/our-work/digital-crime-and-policing/real-lives-real-crimes-a-study-of-digital-crime-and-policing/

[115] HMIC, Regional Organised Crime Units: A review of capability and effectiveness, 2015.
Available at: https://www.justiceinspectorates.gov.uk/hmic/wp-content/uploads/regional-organised-crime-units.pdf

[116] HMIC, Regional Organised Crime Units: A review of capability and effectiveness, 2015.
Available at: https://www.justiceinspectorates.gov.uk/hmic/wp-content/uploads/regional-organised-crime-units.pdf

[117] HMIC found that there was scope for improving the capacity and capability of ROCUs to deliver better results in relation to cyber crime. Source: HMIC, The Strategic Policing Requirement: An inspection of the arrangements that police forces have in place to meet the Strategic Policing Requirement, 2014.
Available at: https://www.justiceinspectorates.gov.uk/hmic/wp-content/uploads/2014/04/an-inspection-of-the-arrangements-that-police-forces-have-in-place-to-meet-the-strategic-policing-requirement.pdf

[118] HMIC, The Strategic Policing Requirement: An inspection of the arrangements that police forces have in place to meet the Strategic Policing Requirement, 2014.
Available at: https://www.justiceinspectorates.gov.uk/hmic/wp-content/uploads/2014/04/an-inspection-of-the-arrangements-that-police-forces-have-in-place-to-meet-the-strategic-policing-requirement.pdf

- Local forces need to be encouraged to better utilise the opportunities that the ROCUs offer for specialist investigative capacity.
- ROCUs should establish a consistent set of operating standards and performance framework.[119] A comprehensive framework would help make them more accountable and effective.

HMIC also noted that 'Home Office funding for ROCUs…is allocated on an annual basis, which makes it difficult for forces to plan for the longer term',[120] suggesting that longer-term funding horizons would also deliver considerable benefits both in strategic and operational terms.

At the national level the NCA is in its very early days. Therefore, it is probably too early to draw conclusions on its effectiveness against cyber crime, however, HMIC noted that improving the communications data capability sharing between the NCA and the security and intelligence agencies would bring benefits to national policing outcomes.[121]

Considerable deficiencies continue to exist at the international level. Yet, as Grabosky and Broadhurst point out, strengthening international initiatives through ensuring there is a framework for international co-operation in place is a vital pre-requisite to dealing with cyber crime, due to its international nature.[122] This is also the most difficult aspect to deal with. Action needs to be global and consequently requires the Government and law enforcement agencies of the countries of the world to more effectively co-operate. There is precedent for the scale of international co-operation and co-ordination needed. The example of dealing with piracy in the 17th and 18th centuries suggests:

> "…a two-pronged approach…The first strategy…to go after the underlying havens, markets and structures that put the profits into the practice and greased the wheels of bad behaviour…the second strategy, the building of a network of treaties and norms…".[123]
>
> Singer, P W and Friedman A, Cyber Security and Cyber War: what everyone needs to know

It is very encouraging that something similar to the first prong of the strategy described by Singer and Friedman was proposed in the Chancellor's speech to GCHQ, along with more funds to help the NCCU operate internationally.[124]

The second prong will require:

> "International agreement on law enforcement and on state behaviour that included restraints on crime…".[125]
>
> Centre for Strategic and International Studies and McAfee, Net Losses; Estimating the Global Cost of Cyber Crime

Grabosky and Broadhurst point out that ensuring existing international treaties are fit for purpose and updated offers the most effective and speediest way to put in place the right international framework.[126] Helpfully there is an international framework for policy makers to build-up and achieve the intensity of co-operation that is needed.[127] This framework includes legal and operational instruments such as the Budapest Convention on Cyber Crime,[128] the UN Convention Against Transnational Organised

[119] HMIC, Regional Organised Crime Units: A review of capability and effectiveness, 2015. Available at: https://www.justiceinspectorates.gov.uk/hmic/wp-content/uploads/regional-organised-crime-units.pdf

[120] HMIC, The Strategic Policing Requirement: An inspection of the arrangements that police forces have in place to meet the Strategic Policing Requirement, 2014. Available at: https://www.justiceinspectorates.gov.uk/hmic/wp-content/uploads/2014/04/an-inspection-of-the-arrangements-that-police-forces-have-in-place-to-meet-the-strategic-policing-requirement.pdf

[121] HMIC recommended that the feasibility of '…opportunities for sharing communications data capacity…' should be explored and then '…be established and begin operation as soon as possible thereafter'. Source: HMIC, In Inspection of the National Crime Agency, 2015. Available at: https://www.justiceinspectorates.gov.uk/hmic/wp-content/uploads/an-inspection-of-the-national-crime-agency.pdf

[122] Grabosky P and Broadhurst R, The Future of Cyber crime in Asia, Cyber crime: The Challenge in Asia, 2005.

[123] Singer, P W and Friedman A, Cyber Security and Cyber War: what everyone needs to know, 2014.

[124] Osborne, G, Chancellor's speech to GCHQ on cyber security, 2015. Available at: https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security

[125] Centre for Strategic and International Studies and McAfee, Net Losses; Estimating the Global Cost of Cybercrime, 2014.

[126] Grabosky P and Broadhurst R, The Future of Cyber crime in Asia, Cyber crime: The Challenge in Asia, 2005.

[127] As is observed in the report Net Losses, Estimating the Global Cost of Cybercrime, international agreements can: '…reduce losses, particularly if this included agreement to observe existing international commitments (such as World Trade Organization [WTO] commitments to protect IP)…'. Source: Centre for Strategic and International Studies and McAfee, Net Losses; Estimating the Global Cost of Cybercrime, 2014.

[128] Council of Europe, Convention on Cybercrime, 2001. Available at: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

Crime,[129] Interpol and a myriad of Mutual Legal Assistance Treaties (MLATs) between countries and Memorandums of Understanding between different law enforcement agencies.[130] The biggest hurdle is generating enough will within the countries and law enforcement agencies of the world to take international co-operation as seriously as domestic law enforcement activity and fully utilising the international instruments available.

Short / medium-term policy recommendations to improve enforcement

Law enforcement should have a central place in the UK's National Cyber Security Strategy and in particular law enforcement aimed at protecting the business community. It should include a commitment to better survey and record the scale of cyber crime against the UK's business community more routinely i.e. as part of the official crime statistics.

The effectiveness of the reporting channels for victims of cyber crime need to be improved. The effectiveness of the forthcoming upgrade of Action Fraud needs to be monitored and evaluated carefully after a reasonable period of time by the Government and HMIC. In addition, the small business community need to be made more aware that Action Fraud is the central point to which they should report cyber crime. Finally, the end-to-end response to cyber crime is poor. The linkages between the national reporting portal and the investigative response at a local and regional level need to be dramatically improved. HMIC suggested that all constabularies should have a responsible senior officer to drive the response from local forces.[131]

The NCA, Police Service and Crown Prosecution Service should develop a fully integrated and comprehensive long term strategy for dealing with cyber crime, encompassing all levels of enforcement and prosecution, which can be proposed in the full knowledge that it will be fully funded. A key aim of the strategy should be to increase dramatically the capacity and capability of the police and prosecutors at local, regional and national level to tackle cyber crime as well as significantly enhancing their international focus.

A key focus of the strategy should be reducing the number of cyber crime incidents against small businesses.

Review sentencing policy towards cyber crime and fraud with the intention of increasing the punishments to act as more of a deterrent.[132]

Long term policy recommendations to improve enforcement

The Government will need to commit more resources to enforcement against cyber criminals. The recent proposed and welcome increases in spending on cyber security (£1.9bn) need to be targeted towards law enforcement. It is likely, however that a further sustained increase in investment will be needed over the long term to get the police and prosecution services to the level where they can effectively tackle cyber crime. This should begin in earnest at the time of the next public spending cycle.

The investment in the police and prosecution services needs to focus on significantly increasing the cyber capability and capacity of police officers, civilian support staff, forensic services and prosecutors.

Ensure that the reforms highlighted by HMIC at the local and regional policing level are implemented. These will require sustained investment over long term horizons and a move away from annual funding of ROCUs. ROCUs have considerable potential but need long-term support to build capacity and capability.

[129] UN Office on Drugs and Crime, United Nations Convention Against Transnational organised Crime And Protocols Thereto, 2004.
Available at: https://www.unodc.org/documents/middleeastandnorthafrica/organised-crime/UNITED_NATIONS_CONVENTION_AGAINST_TRANSNATIONAL_ORGANIZED_CRIME_AND_THE_PROTOCOLS_THERETO.pdf

[130] As illustrations of the MoU's:
One such example is the MoU between the Crown Prosecution Service and the Prosecutor General of the Russian Federation.
Available at: https://www.cps.gov.uk/publications/agencies/opgrf_cps.html
Another is the MoU signed by the City of London Police and US Immigration and Customs Enforcement in 2015.
Available at: https://www.cityoflondon.police.uk/advice-and-support/fraud-and-economic-crime/pipcu/pipcu-news/Pages/Special-relationship-between-City-of-London-Police-and-US-Immigration-and-Customs-Enforcement-%28ICE%29-.aspx

[131] HMIC, Real lives, real crimes: A study of digital crime and policing, 2015.
Available at: https://www.justiceinspectorates.gov.uk/hmic/our-work/digital-crime-and-policing/real-lives-real-crimes-a-study-of-digital-crime-and-policing/

[132] CIFAS have argued in relation to fraud: 'A comprehensive review of the sentencing guidelines for fraud. The public must have faith that when crimes are prosecuted, fraudsters are punished appropriately. And criminals need to know that whether they defraud a multi-national company of millions, or swindle a widower's pension, that they will face a tough sentence which reflects the impact of their crimes'. Source: CIFAS, CIFAS Fraud Manifesto, 2015.
Available at: https://www.cifas.org.uk/fraudmanifesto

The Government should review the relevant law and policy framework to examine whether:

- There are further enhancements that can be made to the law to better encourage co-operation and collaboration between the private sector and law enforcement.
- There can be ways of leveraging in more private sector capacity to deal with cyber crime, including more encouragement of private sector investigation and legal action against cyber criminals.

Grabosky and Broadhurst have described how an effective anti-cyber crime strategy needs to improve the coordination and collaboration (including joint operations) between law enforcement and private sectors through enabling systematic exchanges between them.[133]

There is potential to move beyond collaboration. Given there is considerable expertise and resources in the private sector the Government should review relevant laws and other obstacles which currently might be deterring private organisations from pursuing their own investigations and legal action (civil and criminal) against cyber criminals. As well as removing any obstacles, the Government should look at whether there might be scope for creating specific incentives for encouraging those in the private sector with the expertise and resources into undertaking private investigations and taking private actions against cyber criminals. The objective should be to incentivise additional investigative and enforcement capacity which would complement the efforts of the police and prosecutors.

Once the Investigatory Powers Bill has been passed by Parliament the Government should comprehensively review the current wider criminal and civil powers for dealing with cyber crimes available to law enforcement and relevant regulators (such as Trading Standards).

While the UK is widely considered to have a good framework of criminal law in relation to cyber crime, there may be room for some further enhancements. As Grabosky and Broadhurst have noted, to effectively tackle cyber crime, it is vital that technology and criminal practices do not outpace the ability of law enforcement to investigate and therefore Governments need to be ready to enact substantive and procedural laws which are adequate to cope with current and anticipated manifestations of cyber crime.[134]

While the review should be comprehensive and look to ensure that the barriers to dealing with cyber crime in the UK are minimal, it should include a focus on four issues:

- Reviewing whether the UK is as fully compliant with the requirements of the Council of Europe (Budapest) Convention on cyber crime.[135] Corrective action should be taken where the UK is found not to be fully compliant.
- Look at whether there is any need for creating new criminal offences e.g. a specific offence of ID theft and whether there could be closer regulation of online information sources which make personal information easily available which criminals are able to exploit. One avenue to explore should be whether there is a need for the law to encourage social media sites to be more effective at deleting old data or encouraging their users to make sure they delete old data.[136]
- Whether strict liability offences could play more of a role in dealing with aspects of cyber-criminality.
- The extent to which the tool-box available to law enforcement could be strengthened through the availability of new or the extension of existing civil powers to use alongside the criminal law.

The Government needs to push aggressively the need for more intense international co-operation in all the appropriate international forums, such as the International Telecommunications Union (ITU), the OECD, the UN and the Commonwealth Telecommunications Organisation (CTO) i.e. those international forums that have a truly global reach. Regional measures such as the Network and Information Security Directive are unnecessary distractions and at worst counter-productive complications to the real goal of international co-operation.[137]

[133] Grabosky P and Broadhurst R, The Future of Cyber crime in Asia, Cyber crime: The Challenge in Asia, 2005.

[134] Grabosky P and Broadhurst R, The Future of Cyber crime in Asia, Cyber crime: The Challenge in Asia, 2005.

[135] The Council of Europe's Convention on Cybercrime aims to align the '…relevant criminal laws, police investigative procedures and mutual assistance arrangements of the signatory states'. Source: Wall, D E, 'Cybercrime, 2007.

[136] Tweedie, N, Just how easy is it to hack into your life?, 2011.
Available at: http://www.telegraph.co.uk/finance/newsbysector/mediatechnologyandtelecoms/digital-media/8597757/Just-how-easy-is-it-to-hack-into-your-life.html

[137] FSB argued against the need for the Network and Information Security Directive before it was agreed by the EU institutions. It not only fails, because it is a

The UK Government should put more resources into working with and helping those police forces in less developed parts off the world to build up their enforcement and prosecution capabilities and capacities.

Cyber criminals, like the pirates of the 17th and 18th century, thrive in less well governed spaces, such as countries where law enforcement is relatively weak. More effective police forces and judiciaries in more countries will make it easier to co-operate with the police and judicial authorities across the globe.

Encourage more countries to sign the Budapest Convention. The Convention is currently the preeminent international instrument for fighting cyber crime and needs to be built-up.

The Budapest Convention, along with a network of MLATs, are important elements in creating an international framework for dealing with cyber crime and getting states to put in place the right laws and co-operative practices. However, far too few states are signatories to the former, in part because of its regional origins. It may be that the Convention needs to be re-cast under the auspices of the UN, rather than the Council of Europe, in order to attract more signatories. Signatories should not be afraid of reviewing and refreshing the Convention in light of technological developments. The Government should argue for a regular review of the Convention along with an international push to encourage more states to sign-up and ratify it.

In order to encourage more countries to sign-up to the Budapest Convention, review whether the Government should support it becoming a UN instrument as a complement to the Convention Against Transnational Organised Crime.

Review the UK's current stock of MLATs and Memorandum's of Understanding with the Governments of other countries and their law enforcement agencies where possible. The review should be conducted with the intention of implementing a programme for strengthening them where weaknesses are found.

regional instrument, to deal with many of the risks and sources of the vulnerabilities of the digital economy but did not respect the principle of subsidiarity. It adds in a regional layer of action on cyber-security which creates additional co-ordination problems and needless complications into a system that requires a flat and networked framework to facilitate world-wide co-ordination. When it comes to implementation the Government should work to minimise the scope and impact of the Network and Information Security Directive in the UK. Source: FSB, Network and Information Security Directive: position paper, 2015.

METHODOLOGY

Verve, on behalf of FSB, surveyed FSB's Big Voice Community about the impact of crime on their business between 11- 18 January 2016. The survey had 1006 completed responses.

The questionnaire consisted of 12 questions asking members (among other things) about their priorities and perceptions on business and cyber crime. The questions addressed a smaller firm's experience of being a victim of crime, the extent they report crimes, the cost of the crime and what prevention measures they have in place.

In addition, this paper uses desk research of a range of secondary sources and through discussions with a range of key sources over the past 12 months. These sources included Government Departments (DCMS, Home Office and BIS), academics, cyber security professionals as well as police officers. Key desk research is referenced in the footnotes.

fsb.org.uk

federationofsmallbusinesses

@fsb_policy

If you require this document in an alternative format please email:
accessability@fsb.org.uk

This report can be downloaded from FSB website at www.fsb.org.uk

Experts in Business