TheCityUK

MARSH

CYBER AND THE CITY

Making the UK financial and professional services sector more resilient to cyber attack

May 2016

FOREWORD By John McFarlane

Cyber threat is often talked about as a future risk, suggesting that businesses have the luxury of time to act. That is not my experience. Cyber crime is a real and present danger and financial institutions are on the front line. The very things that customers value – round-the-clock access to their money, single sign-on, one-click purchase – have created new paths for criminals and shared dependencies for the financial system. We in the financial and related professional services sector need to act with the urgency of knowing that a large, systemic risk is upon us. That means individual firms acting to make themselves safe and ready to recover. It also includes the industry acting collectively to make the system safe.

The Government has stepped forward with its recent decision to form a National Cyber Security Centre and to go on the offensive against cyber criminals. We, the industry, need to match that commitment. TheCityUK occupies a unique position in representing firms across the financial and related professional services sector. We hope to use that position to provide a catalyst for having the financial and related professional services sector lean in on cyber, with some practical actions that individual firms and the sector as a whole can take to raise our cyber security.

Finally I would like to thank Mark Weil for chairing TheCityUK's Cyber Taskforce and producing this report, and Marcus Scott for leading the work at TheCityUK. I would also like to thank Marsh and Oliver Wyman for their pro bono support in researching and writing this report.

John McFarlane

Chairman, TheCityUK and
Chairman, Barclays

FOREWORD By Mark Weil

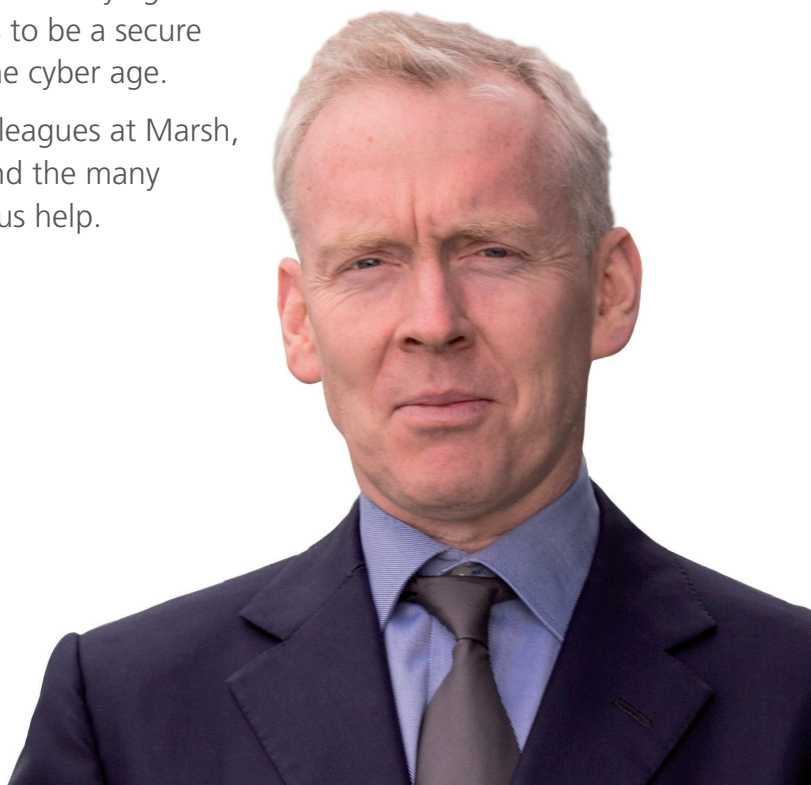
Cyber risk attracts a lot of headlines. It deserves it. In the 2007 credit crisis – a once-in-a- generation event – not one UK bank failed thanks to the simple, fast-acting remedies of cash and capital injection. In contrast, a large-scale cyber attack that renders bank systems or data unusable has no such quick fix for a finance minister or central banker to deploy.

There is a second parallel with the credit crisis. In the run up to 2007, there was a sense in some banks that credit was the concern of technical departments armed with statistical models allowing leaders to be found without a background in banking who could simply focus on growth. When the crisis hit, the banks that did best were those for whom credit-risk awareness was baked into their culture, with a shared appreciation of risk across their leadership and front-line staff.

Cyber risk will follow the same path. At the moment, it is a risk that sits outside of the experience of most leaders in the financial and related professional services sector and is handled by specialists. Technology is now so critical to financial firms that the opportunities and risks it brings need to be central to the running of the firm. Financial firms are in essence a technology-enabled ledger. The data they hold needs to be as familiar to their management as their credit or insurance book; their technology risk as familiar as their credit, market or investment risk.

The UK Government and its agencies have already started to take action. However, outside of a very few firms, we do not yet see cyber getting the attention it needs from business leaders. We seek to build on the progress already made, to give the leaders of financial institutions a basis for staying ahead of the criminals and to make sure the UK continues to be a secure base for the world's leading financial centre in the cyber age.

I would like to thank the taskforce members, colleagues at Marsh, Guy Carpenter and Oliver Wyman, TheCityUK and the many other contributors to this report for their generous help.



Mark Weil

CEO, Marsh Ltd and
Chair of TheCityUK Cyber Taskforce

1.0 SUMMARY AND RECOMMENDATIONS

The financial sector – that tapestry of banks, insurers, asset managers, markets, technology and advisory firms – is a perfect target for cyber crime. It has the data and money to attract criminals, the public profile to attract hactivists and the criticality to the economy to attract terrorists and hostile states. Through a cyber lens, its firms are vehicles for data storage and transmission with a balance sheet attached. They rely on customer confidence which is as vulnerable to repeated data loss, fraud or outages as it is to a credit crisis. Even short- duration accidental ATM and mobile banking outages make the headlines, demonstrating how reliant customers now are on the smooth working of the electronics within the financial system and how sensitive they are to any interruption.

Our economic reliance on trade, inward investment and the financial and related professional services make it critical that we provide a secure place to conduct business. In recognition of that fact, a lot is being done by Government and supervisors on cyber resilience. There is an alphabet soup of bodies and initiatives whether partly or wholly with a financial and related professional services sector focus – CBEST, CREST, CMORG, CPNI, CISP – to reference just some of the Cs. The Government has also recently announced the creation of a National Cyber Security Centre.

This report seeks to build on the good work already done with recommendations for practical steps financial firms can take individually and collectively to improve their cyber resilience, working in partnership with the Government, regulators, supervisors, police and intelligence services. It seeks to align those steps with existing initiatives to avoid adding to an already busy cyber agenda.

We start by defining the problem. Cyber is not an event. It is a conduit for events to occur. That makes the cyber threat broad in nature from minor cases of fraud targeting individuals to sophisticated attempts to destabilise whole firms and economies. To make it actionable, it is therefore important to categorise the different threats and consequences to help pin-point different responses. Cyber risk can be defined as "any risk of financial loss, disruption or damage to reputation from some form of failure of information technology systems."[1] This includes accidents as well as attacks. Our focus is on attacks as these are the majority of the risk and cost.

As a simplification, we categorise attacks into three levels:

Fraud

This covers the majority of cyber incidents today. It includes attempts at extortion, identity theft and other crimes targeting individual customers or employees. The motive is almost always financial. 75% of fraud is now estimated to be cyber-enabled; crudely put, yesterday's 'scam' letter has become today's phishing email. Sums can be large (for example requests for firms to pay fraudulent invoices, or campaigns to steal many people's data) and painful for those affected, but are rarely existential for the firm. While surveys put the average annual cost of cyber crime to large firms at just £1.5m – £3m, this number is likely to be far short of the actual cost, particularly given the concentration of fraud costs in the banking sector. The cost will also be amplified by the sanctions for data breach in recent EU rules. Most financial firms have fraud and security teams; the priority is to adapt them to cope with cyber-specific crime. On the basis that most cyber crime results from basic human error, there is also a need to broaden attention from technology to supplier, employee and customer controls. That should include encouraging customers to take sensible precautions and to encourage a balance of responsibility for the costs when they fail to do so and fall victim to crime, so as to avoid moral hazard.

Firm take-down

This reflects the more ambitious goals of large-scale data theft, system disruption and damage, in which a particular firm is targeted for personal or political reasons. The perpetrator may be a hostile state, terrorist, anti-capitalist, disaffected employee or simply a mischief-maker. Several such cases in the UK and around the world have made the headlines. While few firms of size have so far failed because of such an attack (Nortel is one case of note), the costs and consequences for reputation can nevertheless be severe and it is within the bounds of plausibility that a financial firm – critically reliant on customer confidence – might fail were it to suffer a large or repeated set of such attacks. The wide range in damage from managing through such attacks demonstrates the difference that good preparation makes. Boards need to ensure that management are doing sensible things to reduce the risk and impact of the risk and are prepared to manage a breach.

[1] Institute of Risk Management, 2015

System failure

This covers an incident affecting multiple institutions, for example a concerted attack on several firms, the failure of the payments system or a failure of the national infrastructure that the financial sector relies on such as the power grid. Financial institutions also carry secondary exposure to attacks on sectors where they have balance sheet positions. These 'blackout' or 'cyber hurricane' scenarios naturally get a lot of attention given the extreme consequences – as a parallel, the cost to the Greek economy of the planned shutdown of its banks for three weeks in 2015, is estimated by the IMF to be 7% of Greek GDP. There are, fortunately, a limited list of actors who have both the motivation and the capability to carry out such an attack. Much of the agenda here sits with industry bodies and supervisors to make sure that critical infrastructure and pathways are well protected and that communication, contingency and rapid recovery plans are in place. Its importance to the sector means that the financial industry as a whole should lean in to make sure that enough is being done.

The recommendations in this report follow from this assessment. They reflect interviews with a diverse set of City institutions and authorities, our analysis of the state of play on cyber risk management and our experience in responding to other risks with the potential for extreme impact such as natural catastrophe and terrorism. Recommendations are aimed at one of two audiences:

- The leaders of individual firms in seeking to make their firm safe
- The financial sector as a whole in seeking to make the system safe.

With respect to risk in individual firms, there is still a gap in how seriously cyber is being treated outside of a few firms. In a recent survey of large UK firms, only 50% have cyber in their top ten risks, only 30% have tried to quantify their cyber exposure and only 25% have a cyber incident response plan. Tellingly, only 20% have broader functions engaged in it, suggesting it is being treated as a technology issue. That ignores the fact that a significant number of cyber attacks can be traced back to employees or suppliers who sit within the technology perimeter. In other words, people and processes matter as much as technology.

The good news is that cyber risk lends itself to Board governance in the same way as any other risk. There is no need to reinvent enterprise risk management. Rather, we recommend that Boards conduct regular reviews to ensure that management has taken ownership of the cyber threat. That should ensure that cyber risk is seen as part of business leaders' role and is addressed in a wide range of contexts such as strategy, acquisitions and appraisals. This will widen the functional engagement in cyber risk management from the CIO or CISO to business unit leaders, HR, Risk, Finance, Legal and others.

To encourage such action, we advocate a ten-point check-list for the board to put to management.

Board Cyber Check-List

01	The main cyber threats for the firm have been identified and sized
02	There is an action plan to improve defence and response to these threats
03	Data assets are mapped and actions to secure them are clear
04	Supplier, customer, employee and infrastructure cyber risks are being managed
05	The plan includes independent testing against a recognised framework
06	The risk appetite statement provides control of cyber concentration risk
07	Insurance has been tested for its cyber coverage and counter-party risk
08	Preparations have been made to respond to a successful attack
09	Cyber insights are being shared and gained from peers
10	Regular Board review material is provided to confirm status on the above

Following this check-list does not guarantee safety. On the other hand, an estimated 95% of attacks succeed as a result of basic human error. That supports the Government's claim of an 80% reduction in breaches from following its Cyber Essentials scheme (point 5 above). Equally, the very different experience of firms from similar breaches – some quietly managing through, others being caught up in a media storm – demonstrates the importance of good preparation to stopping a problem turning into a crisis.

With respect to system stability, a lot is being done by the Bank of England, bodies such as CREST and the use of the CBEST framework. The larger banks, amongst others, have responded to their message. We see value in the industry establishing its own body to ensure broader and committed participation on cyber as a complement to supervisory initiatives. Accordingly, we propose that the financial sector sets up a **Cyber Forum** comprising a steering group of Board level cyber risk owners and a working group from the Risk or CISO community. That will allow the industry to mobilise itself around its own defence and to reinforce the goals of Government. Practically speaking, that can be achieved by establishing the Cyber Forum as a committee of TheCityUK, linking to any sector specific equivalents in BBA, ABI and other trade bodies. The Cyber Forum can then take on as its agenda the points below:

- **Encourage information-sharing**. This is an important way to make the attackers' job harder. The large banks already share data via FS-ISAC. The aim should be to encourage more use by others of existing platforms, in particular CISP, as well as creating a forum for broader forms of sharing such as best-practice cyber management. Information-sharing works when contributors get something back – a committee structure will create peer pressure to contribute which will in turn make contributing more worthwhile. It will also help identify any barriers to contribution (such as customer anonymity or regulatory reaction) that need resolving. The information-sharing should be within the sector, but with links to and from the police and intelligence services to support offensive action against criminals.
- **Engage with the regulators** by putting forward guidelines for cyber assessment. Regulators have encouraged large banks towards the NIST framework. Many firms have made progress on scenario identification, quantification and response, which can form more general guidelines for how to manage cyber risk. The fast-moving nature of cyber risk means that guidelines are likely to be more effective than rules or a prescription to adopt one particular framework.
- **Engage with the Bank of England's work** on systemic risk management and in particular on continuity of service, given that the most likely large-scale impact from a cyber attack is the inability of one or more firms to support their customers. Individual firms do, of course, have recovery plans and in-built system redundancy. A sector-wide response might look at issues such as protecting critical shared pathways that have systemic vulnerability, data-portability, dual accounts or other methods for ensuring that an attack does not have widespread implications. There are unlikely to be easy answers (dual accounts, for example, create as many problems as they solve), but reducing outage risk and duration tackles the major systemic threat from cyber.
- **Investigate cyber risk aggregation** in the financial system and the wider economy. Unlike many other risks – terrorism, flood, pandemic to name a few – cyber is not bounded by physical location and circles on a map are no indication to how an attack may spread. That makes it critical to those taking cyber risk, whether directly as an insurer or indirectly as a creditor and investor, to try and bound the aggregation of risk in the economy from widespread attack.
- **Support the development of a UK cyber security sector.** The Government has announced the creation of a National Cyber Security Centre (NCSC) with two cyber innovation centres. The industry should mirror that commitment, starting now in advance of the NCSC. The Cyber Forum should seek opportunities to co-invest with Government in areas such as academic positions, apprenticeships, mentoring, the Cyber Streetwise initiative and the use of start-up firms. That should include trade fairs between City firms, start-ups and incubators such as CyLon and Level 39 to raise awareness and create connections to new firms as well as working with Government to increase exports. Much of this can be done by making time and assets of the financial sector available for this purpose.

- **Increase the pipeline of cyber skilled employees.** Further to the Government's announcement of the creation of the NCSC, work to increase cyber security apprenticeships and the cyber security education programme for 14-17 years olds.
- **Encourage the wider adoption of existing cyber hygiene standards and schemes.** Support and become a "partner" of Cyber Streetwise using existing communications channels to help spread cyber security advice and guidance. Require all suppliers and their supply chains to have Cyber Essentials (or other accreditation such as ISO, NIST) as a minimum.
- **Encourage the adoption of cyber standards in credit and investment decisions.** Financial firms carry an exposure to the firms they support on their balance sheets. That gives them an opportunity to promote cyber security by encouraging firms to make themselves safe. We note that Legal & General, for example, makes cyber security (along with diversity) a part of its investment criteria. The forum should look at how different financial sectors can promote cyber security in their core activities.

Stepping up in this way will add cost. For recruitment, there is an opportunity for firms to get ahead of the apprenticeship levy starting from 2017. More generally, there is a case that the financial sector investing in cyber security will make the UK economy more robust and help to seed a cyber security sector. Given the urgency of the need to get ahead of the risk, one possible way to stimulate activity is to allow for cyber investment to be off-set against industry specific taxes such as the bank surcharge and insurance premium tax. The industry should explore this with the Government on the back of a more specific plan for investing in cyber security.

Our summary recommendations are set out below. They fall into two categories:

Recommendations to individual firms

- Make cyber risk a standing item on the Board or risk committee agenda
- Ensure cyber risk is a part of strategy, investment cases, acquisitions and appraisals
- Have a broad based team inputting to how cyber risk is managed
- Monitor cyber readiness against the ten-point cyber check list.

Recommendations to the financial sector

- Set up an industry-wide Cyber Forum for major institutions to complement existing bodies and initiatives
- Work on systemic cyber risk reduction – information and best practice sharing, risk aggregation and sector resilience
- Encourage support for the UK cyber security sector including apprenticeships, mentoring, access to test facilities and participation in trade events
- Encourage the adoption of cyber standards in lending, underwriting and investment decision to promote cyber security in the wider economy
- Make the case for cyber spend to be off-set against industry-specific costs taxes or levies as a way to catalyse private sector investment in raising system security.

The report gives detail behind these recommendations. They do not cover every aspect of the cyber agenda. Technology is everywhere, is moving fast and is transforming how we work, how crime happens and how wars are fought. For the financial sector, cyber attack is a new source of systemic risk, as much as market or credit risk. That fear needs to be converted into practical steps that firms now take to make themselves and the system safe.

We encourage you to join the debate. A forum for comment will be established, and inquiries, comments, or approaches for collaboration can be directed to cyberandthecity@marsh.com or to TheCityUK at cyber@thecityuk.com

2.0 INTRODUCTION

Technology risk can be defined as "any risk of financial loss, disruption or damage to reputation from some form of failure of information technology systems."[2] Cyber risk relates to attacks which are more likely to be disruptive given their intent to harm. One might also expect increasing technology investment to gradually reduce the level of accident whilst increasing the possibility of attack. The steps taken to manage attacks will anyway be valuable to accidents, for example in preparing for rapid recovery.

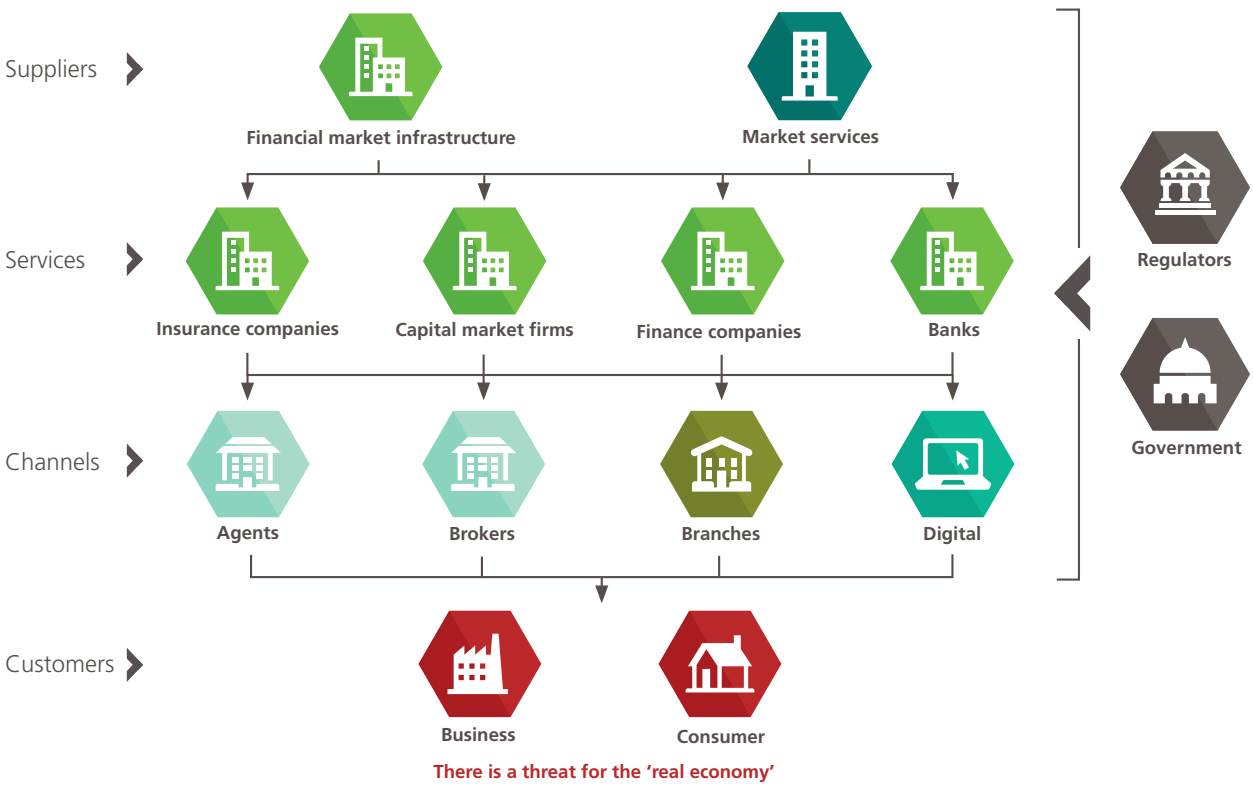
The financial sector comprises many different types of business. Broad categories such as banks or asset managers themselves divide into firms with very distinct types of business.

The financial sector is an important focus for cyber security for several reasons:

- It is an important part of the economy in its own right – including related professional services it accounts for over 10% of UK GDP, employs nearly 2.2 million people and contributes £72bn to the trade balance.
- Financial firms in our assessment score highly on attractiveness to attackers and vulnerability to attack – they are often large, complex organisations with many distributed employees, legacy systems, sensitive data, financial assets and prominent brands. Their inter-dependence also makes them uniquely vulnerable to systemic attack.
- Financial firms are critically dependent on electronic data and its transmission. Disruption to that ability, whether the loss of data or the inability to transmit it,

Figure 1

Illustrative Financial Services ecosystem



Source: Marsh/Oliver Wyman analysis

[2] Institute of Risk Management, 2015

would hamper their operation. The permanent loss of data might even prove an irrecoverable event in contrast to market and credit risk where a financial injection is always available as a remedy of last resort.

- The wider economy also has a critical dependence on financial firms. An attack that prevented people from accessing their bank account, making payments or holding valid insurance would cause disproportionate damage. For that reason, even short duration and non-malicious IT outages at high street banks make headline news.
- Finally, the financial sector offers a way to influence other firms to become more cyber secure. As banks, insurers, asset managers and others adopt cyber requirements into their supply chains and underwriting and investment decisions, it will encourage other firms to raise their own cyber standards.

As part of a report on cyber insurance by Marsh and the Cabinet Office in March 2015[3], TheCityUK was asked to lead work on how best to develop cyber risk capabilities to protect and grow the UK financial sector. This report sets out the results of that work. It had three objectives:

1. To characterise the threat facing the City from cyber attack
2. To set out practical steps to respond to that threat
3. To encourage the growth of a domestic cyber security sector

Our research has considered data and information from a large number of public and private sources on the nature of cyber risk and its management, supplemented by around 20 interviews with cyber professionals in Government and business.

We are also conscious of the amount of activity already going on around cyber. As far as possible, we have tried to build on existing initiatives and thinking with recommendations that will complement these, bringing more support and co-ordination to them.

Alongside the effort going in by individual firms and trade bodies, the UK Government has taken a lead on cyber security. The UK Cyber Security Strategy announced in November 2011[4] identified four objectives:

1. Tackling cyber crime and making the UK one of the most secure places in the world to do business in cyberspace
2. Making the UK more resilient to cyber attack and better able to protect our interests in cyberspace
3. Helping to shape an open, vibrant and stable cyberspace which the UK public can use safely and that supports open societies
4. Building the UK's cross-cutting knowledge, skills and capability to underpin all our cyber security objectives

More recently, in his November 2015 speech, the Chancellor of the Exchequer, George Osborne, set out a plan to create a secure environment for UK cyber activity[5] He announced a doubling of investment relating to cyber security of £1.9bn over five years through five steps:

1. **Improve online defences** with greater efforts to disrupt the criminal marketplace and enhanced capabilities of The National Cyber Crime Unit. Stronger defences for Government systems and public services. Cross-Government IP Reputation Service will be introduced and opportunities to work with Internet Service Providers (ISPs) to provide national protection
2. Greater **coherence with agencies** through a **single National Cyber Security Centre** reporting to GCHQ, building a series of expert teams focussing on industries
3. **Improve cyber skills** to close 2020's 1.5 million security workforce shortage, identifying talent for training and a career in cyber (£20 million competition for new Institute of Coding), introduce more apprenticeships, and improved extracurricular education
4. Programmes to **support the best cyber start-ups**, including **two cyber innovation centres**
5. Respond to cyber attacks with **offensive capabilities** through the The National Offensive Cyber Programme

We support these announcements and have developed this report and the proposed industry response with them in mind.

[3] https://www.gov.uk/government/publications/uk-cyber-security-the-role-of-insurance
[4] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf
[5] https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security

3.0 THE CYBER THREAT

3.1 LEVEL OF THREAT

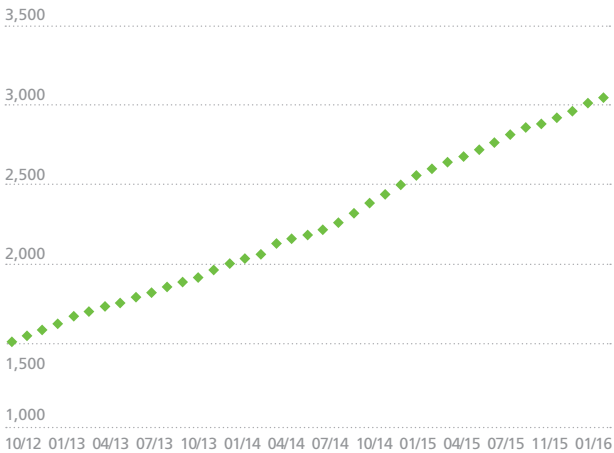
Cyber incidents are increasing in frequency and sophistication as more assets go on-line and as the cost and expertise needed to launch an attack reduces.[7] The number of reported cyber incidents worldwide is expected to grow from 14 billion in 2014 to 24 billion by 2019[8] Similarly, the Index of Cyber Security[9], which uses monthly surveys to aggregate the views of information security professionals, has shown a doubling of the index value in the last three years (Figure 2). Meanwhile, in the Bank of England's December 2015 Financial Stability Report[10], 46% of respondents to their Systemic Risk Survey highlighted cyber risk as a key concern in 2015 H2, compared to just 10% in the same survey a year earlier.

In terms of the particular threat to the financial sector, evidence suggests it receives no more than its 'fair share' of cyber incidents. Other industries including Healthcare, CMT (Communications, Media and Technology) and Retailing are also prominent targets. This ignores the flow of accountability, however, with much consumer fraud (in particular 'card not present' fraud) ending up being paid for by the financial sector.

A more granular assessment of the risk at company level can be done by looking at specific indicators of attractiveness to attackers and vulnerability to attack. Looking across sectors within financial services points to significant differences in risk by type of institution, with banks having the riskiest position (highest motivation for attackers, most vulnerable to attack), followed by insurers and exchanges. These are also the firms with most implications for the wider economy which elevates the importance of cyber risk management to them.

Figure 2

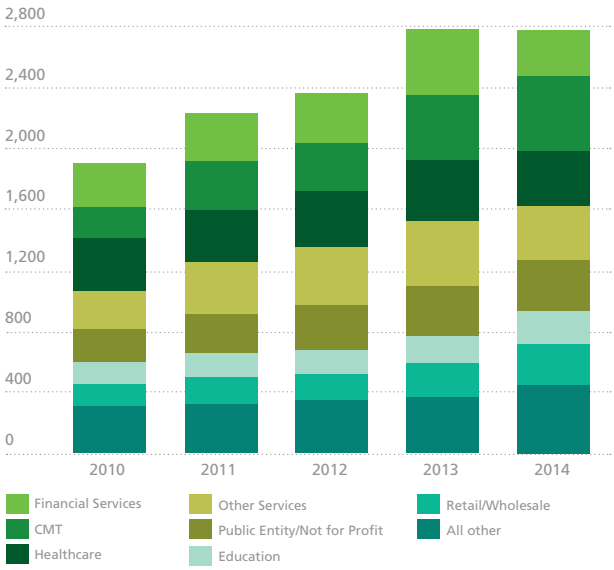
Index of Cyber Security, October 2012 to December 2015



Source: Index of Cyber Security

Figure 3

Cyber incidents per industry



Source: Advisen

[6] Institute of Risk Management, 2015
[7] We focus on threats generated maliciously to information systems originating either externally or internally to, rather than general system/IT failure
[8] http://www.cisco.com/c/en/us/solutions/service-provider/visual-networking-index-vni/index.html
[9] www.cybersecurityindex.org
[10] http://www.bankofengland.co.uk/publications/Documents/fsr/2015/dec.pdf

3.2 TYPES OF THREAT

Cyber is not an event. It is a conduit for events to occur. That makes the cyber threat broad in nature from minor cases of fraud targeting individuals to sophisticated attempts to destabilise whole firms and economies.

Within the complex mix of actors, motivation, method of entry and possible damage, we distinguish three categories of attack as a way to think about the kinds of response needed. These are fraud, firm take-down and system shut-down. It is a simplification, but one which we think helps clarify the issues and actions.

Fraud accounts for the bulk of today's incidents and costs. The ONS reported 2.5 million instances of cyber crime last year. At the same time, the actual annual cost of cyber attacks for large organisations have been estimated at £1.5m to £3m[11]. This figure is likely to understate the real cost, partly through survey bias (lack of willingness to admit to a loss), and partly because of the wider costs such as clean-up that follow attack. It also ignores the concentration of cost in the financial sector from fraud and insurance claims. A bank with a significant payments business might expect an order of magnitude higher costs because of exposure to fraud such as 'card not present' incidents. This nevertheless points to the fact that most cyber attacks today are low level crime and are largely a shift in traditional fraud to a cyber channel.

Most firms have taken steps to protect customers by providing secure channels for mobile or fixed electronic activity. They also often provide guidance on keeping safe from cyber attack. At the same time, the experience of other safety campaigns – seat belts, drink driving, smoking, safe sex for example – suggest that it is a costly, slow process to get messages through even when people's lives are at risk. For the much more intangible and complex cyber risk – often insulated by customers' ability to get financial redress – it will be a long journey. Technology may come to remove the burden from individuals in areas such as biometric identification (the equivalent of driverless cars obviating the need to take driving lessons and wear seat belts), but it is likely that some form of human intervention and hence vulnerability will remain in people's use of technology. The immediate challenge is for firms and the Government to raise awareness of cyber risk and encourage good habits to keep people, whether customers or employees, safe.

Attacks on firms get a lot of prominence when they become public. That may change as the phrase 'cyber' loses its potency to create headlines, but it is likely to stay sensitive for financial firms given the importance of customer confidence to them. For technology and defence firms, theft of intellectual property is a hidden cyber risk which is unlikely to become public, is hard to identify and yet has very high long-term costs. For manufacturers and utilities, damage to property and people is a real concern. For the financial sector, fundamentally engaged in storing and transmitting financial information, the critical concern is large-scale theft, corruption of data and denial of service.

Instances of insolvency due to a cyber attack alone are rare[12] at least for larger firms. Their impact on reputation and customer confidence is still high and would likely be amplified for a financial institution given the importance of customer trust in their integrity.

While there is naturally a tendency to think that the best defence against large scale cyber attack is a strong technology perimeter, human errors and simple systems vulnerabilities continue to be a weakness for many organisations. IBM reports that 95%[13] of all cyber incidents involve human error, and a number of recent high profile events were due to weaknesses in systems, including in their supply chain.[14]

[11] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/432412/bis-15-302-information_security_breaches_survey_2015-full-report.pdf

[12] Nortel, the former Canadian telecoms giant, is believed to have gone bust in part due to cyber, but there were in fact a raft of reasons for its demise

[13] http://www-03.ibm.com/security/services/2014-cyber-security-intelligence-index-infographic/index.html

[14] IBM identifies common errors such as "system misconfiguration, poor patch management, use of default user names and passwords or easy-to-guess passwords, lost laptops or mobile devices, and disclosure of regulated information via use of an incorrect email address"

In thinking about these attacks, culture and process are as important as technology defence; one study[15] found that 73% of companies have been affected by internal information security incidents and that the largest cause of confidential data losses is employees (42%). Employees sit inside the technology perimeter and require a broader approach to managing the cyber risk they create. That may support claims around the value of more comprehensive steps to cyber security such as Cyber Essentials, which claims to prevent 80%[16] of breaches.

Attacks on the financial system have not, so far at least, been successful. The motivation to destabilise the system is less obvious for criminals and more the domain of hactivists, terrorists and hostile states. Taking down a financial system requires a high degree of sophistication for uncertain result versus more traditional forms of terror. Equally, hostile nations are unlikely to engage in such a provocative action outside of the confines of a state of war. That suggests few actors with the motivation and capability to carry out such an act outside of times of war. A notable case was the take-down of Estonia's internet in 2007[17] attributed to actions by the Russian state (Figure 4). Nevertheless, countries such as Israel and South Korea, both with hostile, cyber-capable neighbours have not had any such attacks sufficient to impact their economies, which may point to the difficulty of carrying them out.

Were such an attack to occur, it would have a large cost to the economy. It therefore merits defensive action even though improbable. Sizing the cost of a city-wide attack is very hard, not least because the costs are highly dependent on the nature and duration of the impact, from data loss, to large scale theft to capital market outage. One obvious scenario is the temporary inability of the banks to operate, for example because of the widespread loss of data or disruption to the payments system. The planned closure of Greek banks for three weeks in 2015 (for liquidity rather than cyber reasons) had a similar effect of preventing customers accessing their bank accounts, albeit with more

Figure 4

Attacks against Estonia, April-May 2007/8[18]

Estonia has the highest broadband connectivity in Europe. In 2007, 98 percent of all bank transactions in Estonia used electronic channels and 82 percent of all Estonian tax declarations were submitted through the Internet. Nearly every school in Estonia uses an e-learning environment, and the use of ID cards and digital signatures has become routine in both public and private sector administrations in Estonia.

Estonia has a significant ethnic Russian population, and the movement of a statue of a Soviet soldier commemorating the end of World War II led to civil unrest within Estonia and complaints by the Russian Government. Online DDoS attacks began to target Estonian Government and private sector sites, including banking institutions and news sites.

The attacks built up over the course of a few weeks and peaked at 11 pm Moscow time on Victory Day, 9 May. The attacks hit many parts of the infrastructure, including the websites of the prime minister, parliament, most ministries, political parties, and three of the biggest news organisations. Members of the Estonian Parliament went for four days without email. Government communications networks were reduced to radio for a limited period.

Financial operations were severely compromised, ATMs were crippled, and Hansabank, the largest bank, was forced to close its internet operations. Most people found themselves effectively barred from financial transactions while the attacks were at their height. Estonia responded by closing large parts of its network to people from outside the country, and a consequence was that Estonians abroad were unable to access their bank accounts.

[15] http://www.kaspersky.com/about/news/product/2015/The-Threat-Within-3-Out-Of-4-Companies-Affected-By-Internal-Information-Security-Incidents
[16] Matthew Gould, former Director of Cyber Security and Information Assurance at the Cabinet Office, speaking at Marsh's 8th Annual Client Conference on the 24th November 2015
[17] A good overview of this type of attack is provided by NATO - http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm
[18] http://www.publications.parliament.uk/pa/ld200910/ldselect/ldeucom/68/6805.htm#a3

warning than would be likely from a cyber attack. The IMF and Forbes estimate that the overall impact of this closure on the banks themselves was £12.5bn[19] to £25bn[20], or 7% to 14% of 2014 GDP. That might overstate the impact given the many other stresses in the Greek economy at that point (although unlike a cyber attack, the outage was scheduled and so people had due warning), but does indicate that system outages are costly. That may explain the headlines created by even short duration ATM or mobile banking outages amongst UK clearing banks. By way of contrast, the largest insurance pay-out to date is £51bn in 2005 for Hurricane Katrina[21].

3.3 REGULATION[22]

A significant aspect of the threat is the regulatory consequence of an attack getting through. Large penalties can be incurred, in particular the provisions of the EU's General Data Protection Regulation which allow for fines of up to 4% of global turnover.

We consider the UK and wider European environment, where Trans-Atlantic data privacy is of particular worry, as well as the major initiatives and legislation in the United States where the class action litigation environment creates additional worries for organisations suffering attacks. Noting the severe practical implications, a more joined-up approach would be hugely beneficial. With cyber legislation still evolving, there is a role for financial institutions to increasingly play a role in shaping its development; many issues regarding data have wider ranging implications, for example in the potential use of global distributed ledgers taking advantage of blockchain technology[23].

3.3.1. Cyber regulation in the United Kingdom

The major relevant data environment is under the remit of the Information Commissioner (ICO) who is responsible for enforcing the Data Protection Act. Mandatory reporting is not currently in place for losses of personal data or other impacts of a cyber attack (except for Telecoms companies); however, guidance suggests serious breaches should be reported. In addition, the London Stock Exchange requires listed companies to disclose information which could affect their position on the exchange.

There are additional considerations in the UK for the Financial Services sector in particular due to the role of the major regulators, the FCA and PRA. Unlike the ICO, which can implement fines up to a maximum of £500,000, the Financial Services regulators have uncapped fining powers. Furthermore, firms regulated by the FCA and PRA must report incidents which could significantly harm their reputation, which would certainly cover major cyber attacks.

[19] Forbes - http://www.forbes.com/sites/timworstall/2015/07/18/greek-bank-closure-cost-economy-e3-billion-banks-reopen-monday/
[20] IMF - http://www.imf.org/external/pubs/ft/scr/2015/cr15186.pdf
[21] Swiss Re
[22] Much of this section relies on a recent Clifford Chance report - http://www.cliffordchance.com/briefings/2015/06/cyber_security_legalandregulator.html
[23] This issue is raised in a recent Oliver Wyman report 'Blockchain in Capital Markets: The Prize and the Journey'; we have not generally considered the potential applications of blockchain with a view to reducing cyber risk but believe this is an area worthy of thought

3.3.2.
Cyber regulation in the United States

A wide range of actors in the United States have identified cyber risk as a national priority, but different regulators have different priorities which makes developing a response plan challenging for organisations:

1. **National security** – Homeland Security, the FBI, the NSA and the Department of Defence view cyber primarily as a national security issue, and are keen for the private sector to provide them with as much information about hacking activity as possible, encouraging self-reporting
2. **Consumer protection** – The Federal Trade Commission and attorney generals in the 50 states seem to treat banks as perpetrators who need to tighten security rather than as victims; this impacts willingness of firms to disclose attacks, particularly with the background of class action in the USA
3. **Financial services stability** – the SEC and FINRA are willing to be punitive on firms with deficient systems, while working with them on disclosure and other issues

Despite the conflicting interests of various actors, the US has developed a common standard – the National Institute of Standards and Technology – a voluntary set of leading practices focused on critical infrastructure. Further, there does seem to be some progress with a more balanced approach to private and public information sharing; some proposed legislation would provide legal immunity for companies that share cyber information with the Department for Homeland Security, and the recent Cybersecurity Information Sharing Act (CISA) encourages companies to share information on cyber attacks amongst themselves and with Government, but does not make it mandatory to report cyber attacks.

3.3.3.
Cyber regulation in the European Union

The European Union's policy making is driven by its Cyber Security Strategy, which outlines the following priorities for its Member States[24]:

1. Achieving cyber resilience
2. Drastically reducing cyber crime
3. Developing cyber defence policy and capabilities related to the Common Security and Defence Policy
4. Develop the industrial and technological resources for cyber security
5. Establish a coherent international cyberspace policy for the European Union and promote core EU values

Based on this, the European Commission launched a Directive on Network and Information Security (NIS) in 2013 that is seeking to raise the standards for cyber security. As part of the directive, all EU Member States will need to implement the measures, which are expected to come into force in the next two or three years. These have a number of implications, including the likely introduction of compulsory breach notification. The measures are designed with critical infrastructure, such as Energy, Transport and Financial Services in scope; additional compliance and obligations will likely result, and more incidents would enter the public domain at the behest of national authorities. The European Central Bank has advocated support for the aims of the NIS Directive for Financial Services, whilst looking to retain primary oversight on the Eurosystem's payment and settlement systems.

In addition to the above, moves to unify existing data protection regulations under a single law – the General Data Protection Regulation (GDPR) – has a direct bearing on cyber resilience. The limits this may place on the sharing of information deemed to be personal assets – such as IP addresses – could seriously hinder coordinated responses to attackers. Additionally, fines of up to the greater of €20M or 4% of global turnover are possible for data breach.

[24] http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

4.0 FIRM RESPONSE

4.1 READINESS

Firms are now largely aware of the cyber threat and most have taken specific actions against it. There is evidence however that actions are too narrow and not yet treating cyber risk with the seriousness it merits.

Marsh conducts an annual cyber survey amongst risk managers. It shows little difference between financial firms and others. In the June 2015 survey, responses amongst large firms suggest:

- The risk is still not being recognised widely – only 30% of firms have cyber in their top ten risks. That makes it unlikely that cyber is receiving the attention or funding it deserves.
- It is not being treated in a rigorous way – only 39% of firms have tried to quantify their cyber exposure. That suggests that the threat has not been precisely defined which will make responding to it less effective.
- Leaders are relying on avoidance and not planning for a breach – only 30% stated that they have a comprehensive cyber incident response plan. Firms need to be ready for a breach; not being ready is in part why some firms have struggled to cope with a public breach.
- It is being managed as a technology problem – only 35% have broader functions engaged in it. Seeing cyber risk as being about creating a strong technology perimeter ignores the fact that a significant number of cyber attacks can be traced back to human error including employees and suppliers.

This is not true for all firms. The large banks in particular have been through rigorous assessment and stress-testing in conjunction with the Bank of England. It is, nevertheless, indicative of the state of play more widely both for financial institutions and the firms whose risks they are absorbing whether as suppliers or customers.

4.2 CYBER CHECK-LIST

Cyber incidents are one of the few risks with the potential to bring the firm down. Accordingly, we see it as critical that Boards ensure management ownership of the risk, and that the Board shifts the attitude to cyber from being a technology and security issue to being an enterprise risk touching all parts of the firm. This sentiment is now common-place in guidance on cyber governance. The challenge is to turn the sentiment into action, given the newness and complexity of cyber risk and the technical issues and jargon that surround it.

With that in mind, we put forward a 10 point cyber check-list for the Board to challenge management on the treatment of cyber risk. These are designed to cut through the complexity to the salient issues that require action.

Board Cyber Check-List

01	The main cyber threats for the firm have been identified and sized
02	There is an action plan to improve defence and response to these threats
03	Data assets are mapped and actions to secure them are clear
04	Supplier, customer, employee and infrastructure cyber risks are being managed
05	The plan includes independent testing against a recognised framework
06	The risk appetite statement provides control of cyber concentration risk
07	Insurance has been tested for its cyber coverage and counter-party risk
08	Preparations have been made to respond to a successful attack
09	Cyber insights are being shared and gained from peers
10	Regular Board review material is provided to confirm status on the above

We now work through these in turn, giving commentary on each.

01 The main cyber threats for the firm have been identified and sized

Cyber risk will manifest differently for different firms. Firms engaged in trading activity may have exposure to market abuse. Those engaged in payments may have particular exposure to outages. Financial firms are diverse and need to pay attention to what might seem relatively obscure areas of their business but where potentially critical risks are being incurred.

Firms then need to quantify the likely impact of those scenarios playing out. That is hard, but getting easier as the number of historic cases increases and as useful parallels are found from losses not caused by cyber, but with similar consequences. In our experience financial stress-testing, particularly of cash-flow given the acute nature of cyber attack, improves the rigour with which impacts have been looked at as well as quantifying the need for remedies such as insurance.

02 There is an action plan to improve defence and response to these threats

This is the critical outcome. There are few useful KPIs on cyber (volumes of attacks or % of attacks thwarted tell you nothing about future risk). Instead, the focus for Board attention should be the actions being taken to improve defence and reduce impact. The scenarios on which actions are built will not be complete, but the actions will likely help improve cyber resilience in general, not just for the narrow set of scenarios chosen.

03 Data assets are mapped and actions to secure them are clear

Cyber attacks are not all about data theft. But data is often a focus for attackers whether to create embarrassing leaks, to sell on customer financial information, or destroy critical records. CEOs can be expected to have a good grasp of their balance sheet in particular their credit, insurance and investment books, analysis of their performance and insight into their risk. In contrast, few will have a good grasp of their data – what they hold, how it gets used, how secure it is, how it interconnects and who has access (often many thousands of suppliers and employees). Data needs to be seen as a critical asset that is understood in the same way as other assets material to the financial well-being of the firm.

04 Supplier, customer, employee and infrastructure cyber risks are being managed

Each of these has the potential to be the source of the problem, whether maliciously (a disgruntled employee posting sensitive information – think Edward Snowdon) or through contamination (a supplier was the conduit into the US retailer Target).

For suppliers, the firm should ensure that cyber standards are being imposed on the supply-chain to reduce the possibility of third party contamination. There is no set formula for how this is best done, but the expectation of some standards for cyber security such as Cyber Essentials accreditation is a minimum step.

For employees, the issue is around access rights, monitoring of network activity and education on safe conduct. Employees opening the wrong email or visiting contaminated sites can be the conduit for malware just as a supplier can.

For customers, the issue for financial firms is partly around keeping them safe through provision of secure transaction interfaces and, particularly for consumers, through education. Financial firms have the added issue of taking exposure to their customers through lending to, insuring or investing in their business. Cyber security will over time become an important predictor of firm default. We believe financial firms should get ahead of that concentration risk in their balance sheets by putting cyber security, for example cyber standards accreditation, into their core questions such as the bank's credit decision set.

For infrastructure on which the firm depends, there are some actions within the grasp of the firm itself – to identify such dependencies and, as far as possible, plan for failure and recovery. This is an area where collective action is required, and the firm should in part turn its attention to ensuring that the industry and authorities are putting adequate effort into ensuring that critical infrastructure is being protected and that rapid recovery from attack is achievable.

05 The plan includes independent testing against a recognised framework

There are several useful frameworks out there that are built on expert assessment of best practice and which broaden the focus from purely technology to include people, processes and other sources of risk and defence. The large banks, for example, have largely adopted NIST framework, coming out of their co-ordinated actions on cyber security. We stop short of recommending that every firm becomes accredited on a recognised scheme, but do believe that they should use these frameworks as a way to ensure that actions being taken are of sufficient breadth to cover the range of risk factors. Doing that as an independent exercise will bring fresh perspective and credibility to where the firm is at on cyber security.

06 The risk appetite statement provides control of cyber concentration risk

Most financial firms have risk appetite statements. These vary in detail and prescriptiveness, but some statement of concentration limit for lending, insuring or investing will be typical. Traditionally these restrict things like the size of the largest single client, the amount of business to be done in a particular industry or particular country. Cyber risk knows no such boundaries. Its perimeters are defined more by the underlying service and technology providers that clients use and the firms that they trade with. There are tools that map these risks and which can be used to try and bound the danger of aggregating cyber exposure onto the balance sheet.

07 Insurance has been tested for its cyber coverage and counter-party risk

Survey evidence suggests that 50% of CEOs believe that they have insurance cover for cyber attack, whereas policy analysis suggests that only 10% do. That gap is likely a result of the ambiguity in many policies over whether cyber is covered or not both in general and for the scenarios of most concern to the firm. That raises a question over the efficacy of cover for the insured. It also raises a question over counter-party risk given the large possible losses were a systemic event to happen given coverage ambiguity. It requires a review by insured firms of how their policies would respond to the chosen scenarios and corrective action on policy and if necessary insurer to make sure that cover is appropriate. This is a natural extension of the financial stress-testing described earlier, in that insurance cover should be set in the context of the capital and liquidity position required.

08 Preparations have been made to respond to a successful attack

The Board should ensure that the organisation is prepared for the possibility of a successful attack through dry-runs, service recovery plans, communication training and stakeholder management, noting the many bodies that may need managing in the event of an event that may have regulatory, criminal and security implications. Boards should have the comfort that the internal and public response to a cyber attack is not being tried for the first time after a major breach. Recent cases demonstrate in particular the importance of an effective communication approach to retain customer confidence while managing through the issues.

09 Cyber insights are being shared and gained from peers

Sharing information is important to a firm's own defence as well as a public good for the sector as a whole. Contributors will be deterred if they find that they are not getting useful information back. The Board should make sure that it is part of the information pool, both for its own benefit and to encourage information-sharing on cyber risk in general. That should extend to best practice so that the Board has a sense of how it benchmarks against peers, noting the value in being a hard target. There are valid concerns about the nature of information to be shared, such as whether it compromises customers or the firm itself. There are also multiple bodies involved in information-sharing. Some simplification is required to make this easier and we make recommendations to that end in the next section.

10 Regular Board review material is provided to confirm status on the above

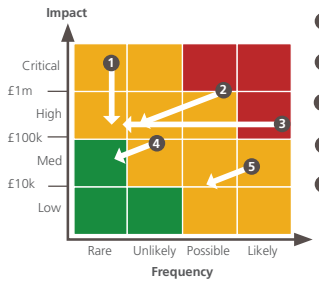
The Board should be seeing important information on cyber risk management. That should focus on progress being made on the points above as well as any major incidents to have happened (or been avoided) in the firm or its peer set. The critical thing is for reporting to be clear, actionable and focused on the measures that will make the firm safer. An example being used for that purpose is shown below. It focuses on the status of specific risk scenarios identified for the firm and progress on actions being taken to mitigate them. The important point to note is that this forces cyber into the disciplines and language of operational risk management to make it supervisable by a non-technical board.

These steps will not guarantee cyber safety. They should, though, make a material difference. The predominance of human error, basic security glitches and employee involvement in the majority of cyber attacks supports the claims for dramatic reduction in risk gained through accreditations such as for Cyber Essentials. To some extent, cyber safety is about displacement. If one firm is harder to attack, it is likely that the attacker will go elsewhere. The same can be extrapolated to a sector, a city and a country. It suggests that measures do not need to be perfect, they just need to make the attacker's job that much harder.

Example Cyber board reporting

Cyber Risk Heat Map

Risk management strategies in place for key risks



	Cyber Risk	Management Strategy
1	• Network infiltration • Customer data loss	• Insurance
2	• Defective system changes • Customer contact data loss	• Process change • Insurance
3	• DDoS attack • Operational disruption	• Vendor solution
4	• Supplier security deficiency • Client card data loss	• Define 3rd party dilligence
5	• Ransomware attack • Extortion	• Training • Insurance

Progress against Cyber Objectives

Progress being made all major cyber objectives

Cyber Objective	Status Against Plan
Cyber threats have been identified and quantified	→
Security improvement programme on track	↑
Data assets mapped and secured	↑
Cyber risk appetite has been defined	→
Cyber risks managed against risk appetite	↑
Cyber security validated against ISO 27001	↑
High degree of confidence in cyber insurance cover	→
Crisis Management plans in place	→
Cyber insights are being shared and gained from peers	↓
Board is updated regularly on cyber risks	↑

5.0 SECTOR RESPONSE

5.1 CYBER FORUM

Cyber security is a public good given the shared nature of the threat, technology interdependencies and reputational interest in the UK and especially the City as a safe place to do business. That view is broadly recognised, and a lot of work has already been done by the Government, supervisors and firms to create a common agenda and push risk reducing initiatives.

This section puts forward a proposal for the financial sector to step forward on this issue, doing its part to take leadership and complementing the many existing initiatives that are going on. Our proposal is for the sector to create its own Cyber Forum. That allows existing activity to continue, but becomes a strong platform for interfacing with industry and Government initiatives. The arguments for the Cyber Forum are that it brings together different parts of the financial sector in a single group, that it can be set up with Board level sponsorship (noting our earlier plea for Board ownership of cyber risk) and that it works to an agenda that covers the critical systemic risks.

We stress that this is to support rather than replace existing initiatives. As a simple example, such a forum is a good vehicle for creating peer pressure to contribute to information-sharing via CISP. There are already informal gatherings of like-minded firms, and actions being taken in particular trade bodies. There are also formal groupings such as CBEST and CMORG mobilised by the Bank of England. We envisage the Cyber Forum adding to these.

We suggest that the Cyber Forum should have Board-level risk representation for a steering committee and CISO or Risk function representation for its working group. It will most efficiently be part of an existing industry body such as TheCityUK.

The Cyber Forum can then take on as its agenda the points below, whether as a leader or to encourage action by supervisors and other bodies:

1. **Encourage information-sharing amongst industry participants.** There are already several forums for information-sharing. We see an industry body as a good basis for creating commitment to use those forums and so increase their utility for all. The alternative to this is mandatory reporting which we see as less attractive as it may (like sanctions) discourage firms categorising incidents as breaches and reduce their willingness to share them.
2. **Put forward guidelines for cyber risk management.** A part of information-sharing should be around best practice and lessons learned in managing cyber risk. Supervisors and legislators are also shaping the landscape and the industry should step forward to help ensure that this is done in ways that are encouraging and effective.
3. **Work on systemic risk management and in particular on continuity of service.** The most serious kind of systemic cyber attack would likely be a black-out, potentially involving a sustained (if not permanent) outage for one or more institutions or systems (such as payments). The industry should make sure that it is getting the attention it deserves given the complexity of issues and competing priorities amongst institutions and supervisors.
4. Work on understanding **cyber risk aggregation**. All financial firms are exposed to risk aggregation. In the case of cyber it is hard to quantify because unlike most other risks it is not bounded by circles on a map. Getting to grips with how cyber risk accumulates in the financial system and wider economy will be a technical break-through of value to all firms whether banks, insurers or asset managers. This is a key part of the work of CMORG and its cyber group (CCG).
5. **Support the development of a UK cyber security sector.** The UK financial sector will be a substantial consumer of cyber risk services. It will be agnostic where these come from, but can play its part in ensuring that London is an attractive hub for talent from around the world. Hosting a major cyber security centre will be complementary to the financial sector as well as a good for the UK economy in its own right. We see value in the industry committing to support mentoring of start-ups, apprenticeships, providing access to dummy data and systems for R&D, supporting trade-fairs of UK cyber innovators etc. This should be done in conjunction with the NCSC and innovation centres as they come on board. At this point, we seek the commitment from senior industry figures to this agenda, with the Cyber Forum providing the vehicle to promote activity in tandem with other bodies.

In each area, a lot has been done and there are some important contextual issues to address. The intention here is to encourage industry-wide participation with senior sponsorship to ensure that the industry helps accelerate actions critical to sector stability. The list is not exhaustive, nor set in stone. It is based on a review of factors raised by cyber experts and management. More detail on the state of play for each issue listed is provided in the sections that follow.

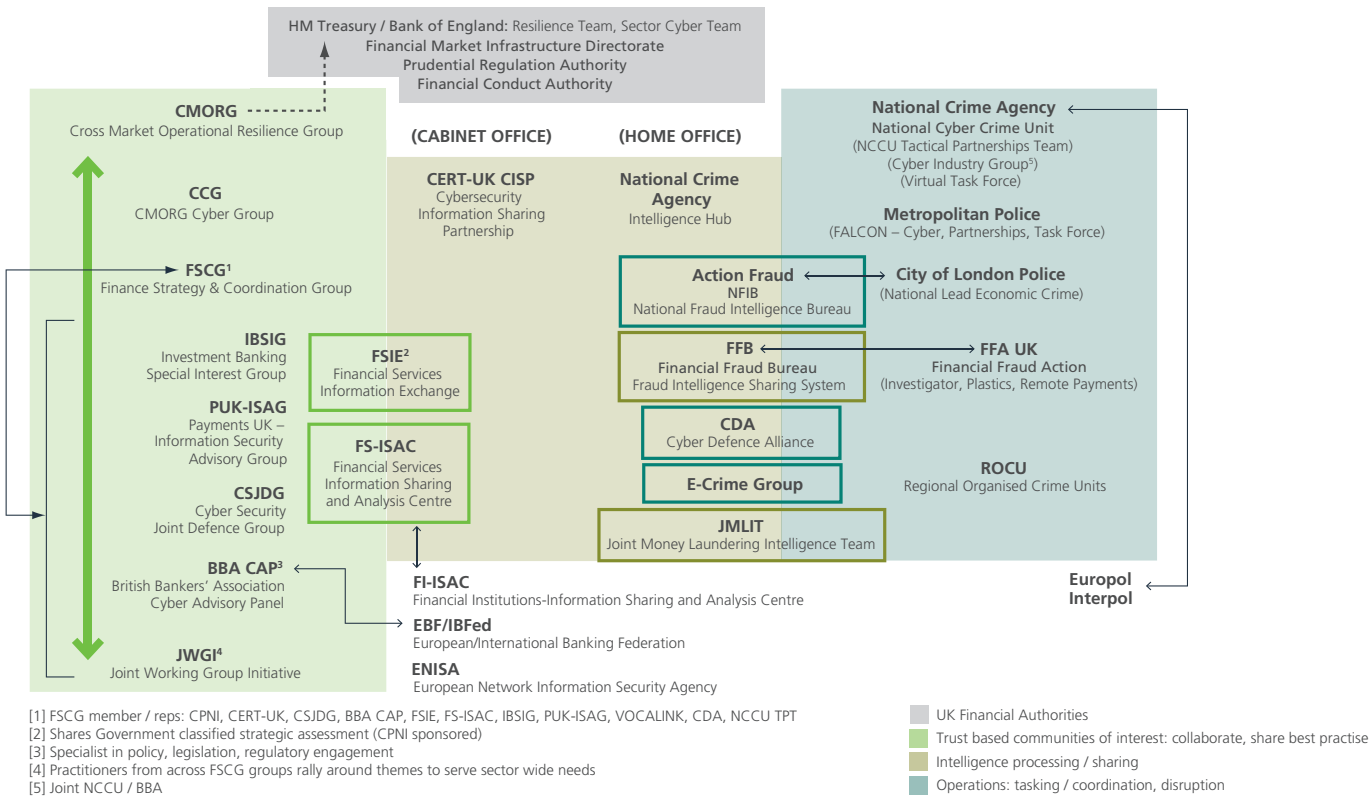
5.2 INFORMATION-SHARING

There are already many bodies that act as a vehicle for organisations to cooperate, sharing experiences and intelligence about existing cyber threats. These offer a variety of ways for organisations to improve their awareness and adopt an intelligence led approach to collaboration over existing cyber threats, as is advocated in research papers by Payments UK[25].

The Finance Strategy and Coordination Group, a body consisting of several finance sector groups (including British Bankers' Association, CERT-UK and Payments UK), has developed a view of the current cyber information landscape:

Figure 5

Current cyber information sharing landscape[26]



Source: FSCG (Finance Strategy & Co-ordination Group)

[25] Payments UK (formerly Payments Council) has produced whitepapers on Cyber Threat Intelligence in April 2014, recommending a collaborative intelligence-led approach for organisations to achieve optimal cyber security

[26] Source: FSCG (Finance Strategy & Co-ordination Group)

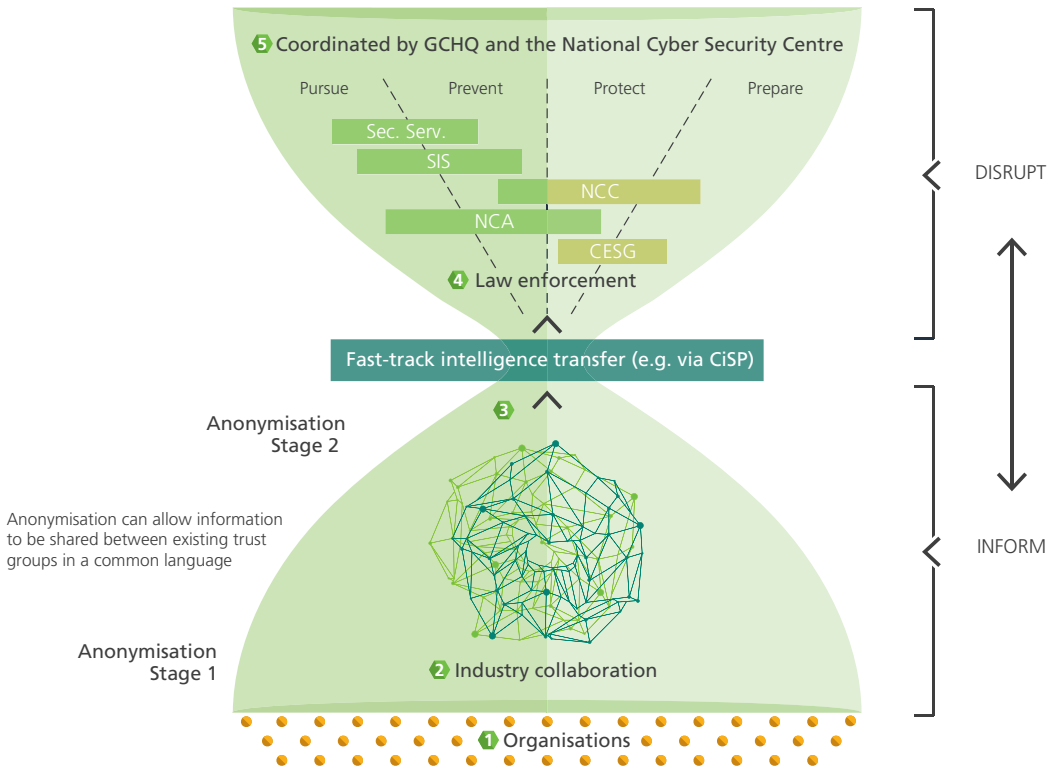
Intelligence sharing should be based on a common set of standards such as STIX (Structured Threat Information Expression) and TAXII (Trusted Automated Exchange of Indicator Information) for sharing technical information, which are technical specifications that enable automated information sharing for cyber security situational awareness, real-time network defence and sophisticated threat analysis. Likewise, when sharing non-technical information, a common language should be adopted for effective communication and response.

Cooperation with law enforcement will ensure that intelligence on breaches and attacks reaches bodies such as National Cyber Crime Unit (NCCU), through which cyber criminals can be brought to justice. Law enforcement play multiple roles in fighting the cyber threat and parallels can be drawn with the UK's Strategy for Countering International Terrorism, whereby law enforcement should look to perform the 4 P's: Pursue, Prevent, Protect and Prepare[28]. Law enforcement is uniquely placed to Pursue, relative to other organisations, and with the introduction of the National Offensive Cyber Programme, effective cooperation can provide the foundation for pre-empting attacks and instead attacking first[28].

Of the five million fraud and 2.5 million cyber-related crimes occurring annually in the UK[29], only 250,000 are being reported. Of these 70,000 are allocated to police[30], leading to 12,000 prosecutions. This demonstrates the critical role that police and law enforcement play in the fight against cyber threats, and underlines the need for a joined-up approach between industry and Government

Figure 6

Recommended information sharing approach



Source: Payments UK

[27] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228907/7833.pdf
[28] https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security
[29] http://www.ons.gov.uk/ons/rel/crime-stats/crime-statistics/year-ending-june-2015/sty-fraud.html
[30] https://www.cityoflondon.police.uk/news-and-appeals/Pages/Adrian-Leppard-Fraud-and-Cyber-crime.aspx

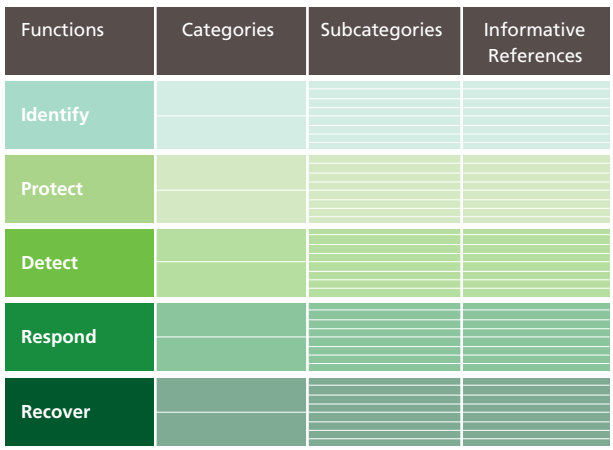
bodies. Incidents are currently underreported, and in order to bring cases to the attention of the police, organisations and individuals should look to report crime and share information that they are aware of more regularly. With more crimes reported, law enforcement will be able to bring more cyber criminals to justice, growing the prosecution rate from 0.16%[31] both domestically and by cooperating with international agencies such as the European Union Agency for Network and Information Security (ENISA) and the US FBI and Department of Homeland Security.

There is always a difficult balance between privacy and security which data-sharing invokes. The recent high profile Safe Harbour[32] case has damaged Trans-Atlantic collaboration, but regulators need to respond to the borderless cyber threat with a more coherent international framework to address the data sharing issues. This may include the reclassification of what constitutes personal data, or a fast and straightforward mechanism to circumscribe data laws in the event of a major attack. These measures would not be popular, but new ideas need to at least be considered to address the problem. At the very least, setting global standards as an extension of the EU Data Protection Directive and Regulation needs to happen sooner rather than later.

5.3 GUIDELINES FOR BEST PRACTICE

There are several guidelines and accreditation schemes for cyber risk. For example, the UK Government has launched Cyber Essentials – a Government backed and industry supported scheme to guide businesses in protecting themselves against cyber threats. The Cabinet Office estimates that 80% of breaches would not occur if the Cyber Essentials advice was taken on board and implemented[33]. However, meeting all the requirements of Cyber Essentials in reality is not a straightforward task and requires organisations to dedicate both time and resources to achieving the criteria. It also stops short of being an enterprise wide solution to cyber risk management, covering issues such as scenario identification, stress-testing and response. Similarly in the US, NIST provides a framework for assessing cyber risk.

NIST Framework Core



It is likely that the UK regulatory community will want to see evidence that best practice cyber risk management is taking place in individual firms, whether from a prudential or conduct point of view. Given the rapid emergence of cyber as a threat, we see an opportunity for the industry to step forward with a view of what good looks like in cyber risk management. That will have value to firms individually and allow the sector to provide a view to supervisors.

We envisage this staying at a broad level of guidelines. It is hard to be prescriptive on particular processes or tools given how different firms are, how fast the threat is evolving and the fact that any fixed approach sets a known bar for attackers to clear.

Taking this approach also offers at least the possibility of super-equivalence for what is done in UK. Firms are seeing other regulators copy aspects of what is being done by UK supervisors (notably CBEST). Running the same tests on the same global operating platform multiple times is costly, and a goal here should be to work with UK authorities to try and win the argument for international recognition of UK cyber assessment.

[31] Calculated as prosecutions relative to cyber incidents
[32] The following paper provides a useful overview - http://www.cliffordchance.com/briefings/2015/10/safe_harbor_declaredinvalidwhatitmeansfo.html
[33] Matthew Gould, Director of Cyber Security and Information Assurance at the Cabinet Office, speaking at Marsh's 8th Annual Client Conference on the 24th November 2015

5.4 SECTOR RESILIENCE

In the area of individual institution vulnerability testing, the UK is already well-placed. The CBEST framework developed by the Bank of England has been finished by 10 core firms undergoing the programme, and a further 35 are in the process of completing it[34]. The Bank of England expects firms at the core of the financial system will take the testing and that "this testing [will] be integrated into regular supervisory activity."

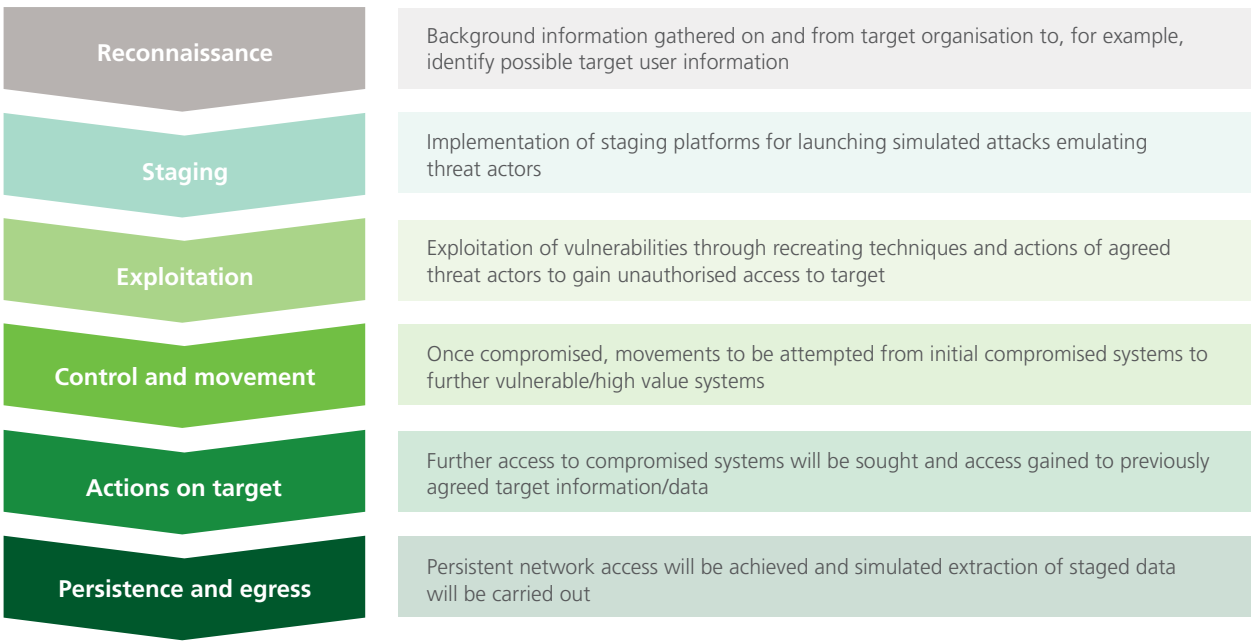
The CBEST vulnerability testing framework seeks to improve and test the resilience of financial institutions to sophisticated cyber attacks. CBEST supports boards of financial firms, infrastructure providers and regulators themselves to better manage cyber risk and understand the vulnerability of the UK financial sector to cyber attacks, as well as assess detection and recovery processes, through the simulation of real-world attacks.

As part of CBEST, the Bank of England and CREST have approved a number of companies to provide CBEST services; additionally, CREST endorses members across a range of service types[35]. Developing a wider list of cyber technological solutions and providing accreditation would be a beneficial step and help organisations more effectively find help when they need it.

CBEST is still in development but is considered an effective tool for assessing cyber resilience – so much so that the United States and Dutch regulators have expressed an interest in purchasing the program[36]. With many organisations dependent on the same systems and enterprise software, vulnerability testing of an organisation is also beneficial for identifying deficiencies that could impact multiple users of a common system, and hence should be a consideration for regulators overseeing financial services firms.

Figure 7

CBEST testing methodology



[34] http://www.bankofengland.co.uk/publications/Documents/fsr/2015/dec.pdf
[35] http://crest-approved.org/crest-member-companies/member-companies/index.html
[36] [Bank of England]

CBEST works at the level of the individual institution. It nevertheless contributes to system stability by making sure large firms are made more resilient. Where it stops short is in questions around critical infrastructure and the vulnerability they create to wide-spread impact, and on the question of recovery from such an attack.

As a broader test of industry response to cyber attacks the Bank of England has coordinated the Waking Shark I and Waking Shark II exercises, whose recommendations to the Financial Authorities included a request for enhancements of the CiSP platform through closer firm and Government collaboration, and for the PRA and FCA to ensure dual-regulated firms are fully aware of incident reporting requirements and update frequencies. Additionally, international collaboration exercises are being introduced, such as Operation Resilient Shield that will look to test Trans-Atlantic communications and coordination under a simulated major cyber attack from the Bank of England and the Federal Reserve.

With respect to infrastructure, mapping is needed to identify non-financial firms and platforms on which the City has particular dependency. These firms – from an operational and cyber risk point of view – may be more important than the failure of any individual financial institution. It raises the question of who they are and what tests they should be put through to ensure cyber resilience. Individual FIs should conduct their own cyber defence exercises (CDXs) to test procedures, acclimatise key decision makers to the rapid nature of strategic decision making in a cyber crisis and develop appropriate lines to take for PR and communications in advance.

With respect to recovery, there are no easy answers. Firms will have disaster recovery plans and sites established, but these will typically have been established more for physical damage than cyber attack – back-up sites and systems may themselves be vulnerable to the primary attack. For institutions whose customers require immediate transaction (most obviously markets and banks), system resilience would be increased if they were able to shift their load to alternative institutions. That is hard to do. For banks, for example, simple remedies such as customers holding dual accounts ignore the fact that an account is only useful if it holds the balances and up-to-date information to transact. We recognise that work is being done on this issue, notably by the Bank of England's Resilience team. We see it as the single most important aspect of systemic cyber risk and want to encourage the sector to ensure that work is getting the attention it deserves.

Joint industry and Government investment in educational initiatives such as the National Cyber Security Awareness Month and Cyber Streetwise should be marketed more widely, and guidance on basic measures, such as having two bank accounts to mitigate the effects of a cyber attack (as recommended by a former adviser to the Bank of England[37]), should be regularly communicated to the general public. Likewise, the work of bodies such as the CPNI that issue guidance on implementing cyber security controls should be continued and encouraged.

[37] http://www.telegraph.co.uk/finance/personalfinance/bank-accounts/12028576/Bank-of-England-adviser-Everyone-should-have-two-bank-accounts-in-case-of-cyber-attack.html

5.5 RISK AGGREGATION

Most operational risks can be bounded in relatively straightforward ways. For example terrorism risk is defined by blast zones which allow insurers to define Possible Maximum Loss for single and multiple incidents. One of the defining features of the credit crisis at its inception was the way risk spread through the system as banks tried to establish who had exposure to the problematic US sub-prime loans. A strong catalyst for the panic that followed was uncertainty over the boundaries of the risk. Cyber risk has the potential to behave in the same way; seemingly independent firms may turn out to share common exposure to cyber risk by dint of common suppliers or customers, or by using common service providers and infrastructure.

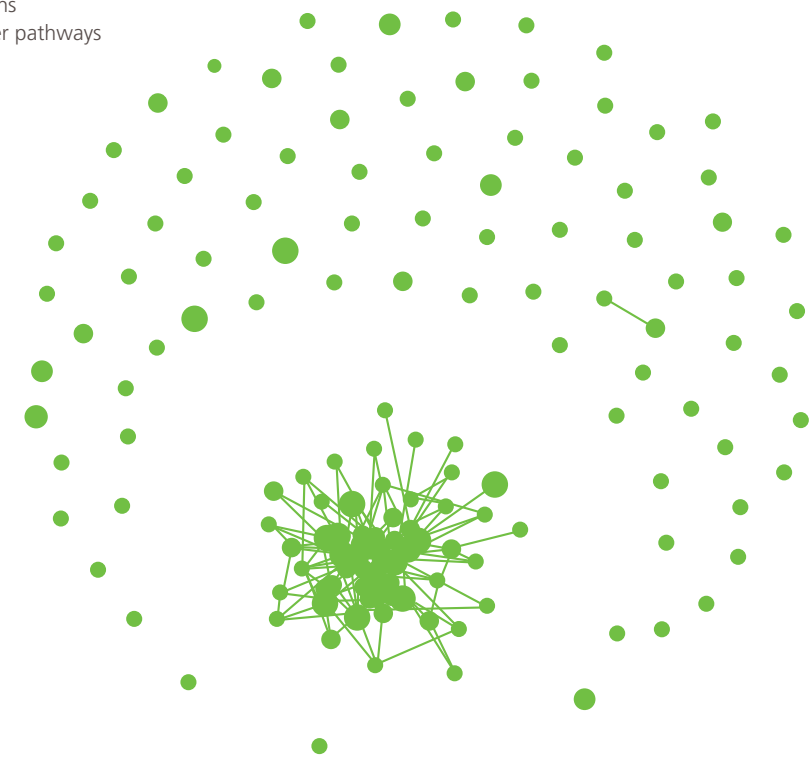
There are tools for mapping cyber risk aggregation. These give at least a basis for starting to address the problem of how cyber risk might accumulate in the financial system via common dependencies and pathways.

The basis for assessing cyber risk aggregation will ultimately benefits customers in that banks, insurers and asset managers can make use of in their individual decisions as well as supervisors in thinking about systemic risk. It will support specific challenges such as the insurance sector's containment of cyber risk so that it can write large scale cyber policies with confidence.

Figure 8

Cyber Risk Aggregation in Large City Firms

Dots = individual institutions
Proximity = common cyber pathways



5.6 DEVELOPING A UK CYBER SECTOR

Cyber security firms already have achieved a substantial presence in the UK, with more than 1,000 organisations spread across the country and offering services that present numerous export opportunities. The Cyber Growth Partnership has compiled an online directory of these organisations, providing a central repository of the UK's cyber security offering[38]. At the start-up end, organisations like CyLon are providing incubation for people from around the world looking to establish a cyber security business.

Figure 9 provides an illustration of a non-exhaustive range of services that some existing UK cyber security firms offer[39]:

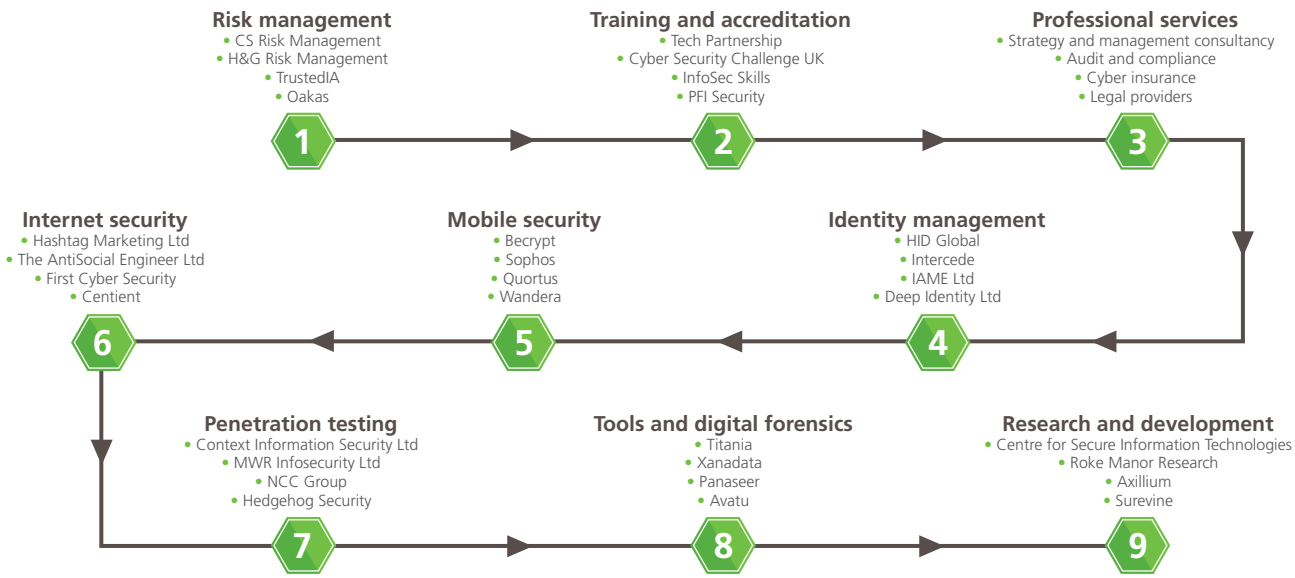
The global cyber security market was valued at ~£50bn in 2015[40] and is expected to grow at a CAGR of ~10% according to some estimates[41]. With UK's cyber security exports making up ~£1.5bn of that in 2014, there is an opportunity to expand in the growing market[42].

Israel-based CyberGym, which provides comprehensive IT security services and real-world cyber defence training, provides a good example of how to develop international cyber centres, launching its European offering in 2016 in the Czech Republic[43].

To ensure the greatest success of this initiative, the Financial Services industry and UK Government should look to cooperate with the UKTI and Cyber Growth Partnership. Existing measures, such as the development of a Cyber Map by the Cyber Growth Partnership that details a directory of over a thousand cyber security firms located in the UK[44], illustrates steps being taken to apply

Figure 9

Illustrative taxonomy of UK cyber firms and their service offering



Source: Cyber Growth Partnership

[38] https://www.cgp.uk.net/#/directory
[39] Referenced organisations do not exclusively provide a single service, with each typically providing a range of cyber security services, including those that are both mentioned and not mentioned in the diagram
[40] http://www.gartner.com/newsroom/id/3135617
[41] http://www.marketsandmarkets.com/PressReleases/cyber-security.asp
[42] https://www.gov.uk/government/statistics/uk-defence-and-security-export-figures-2014
[43] https://www.cybergymeurope.com/
[44] https://www.cgp.uk.net/#/cyber-map

a coordinated approach. The Taskforce supports existing governmental efforts to adopt a cyber export strategy, collaborating with UKTI and building an overseas customer base from targeted geographies such as the Gulf States and South East Asia[45].

There is also a talent gap given the rapid increase in demand for cyber security capabilities and given the high level of training required. There is a lot happening already in the UK through Government initiatives and this should be supplemented by the work of individual firms, such as the provision of apprenticeships and work placements required for trainees to acquire the hands-on experience they need to move into cyber security roles.

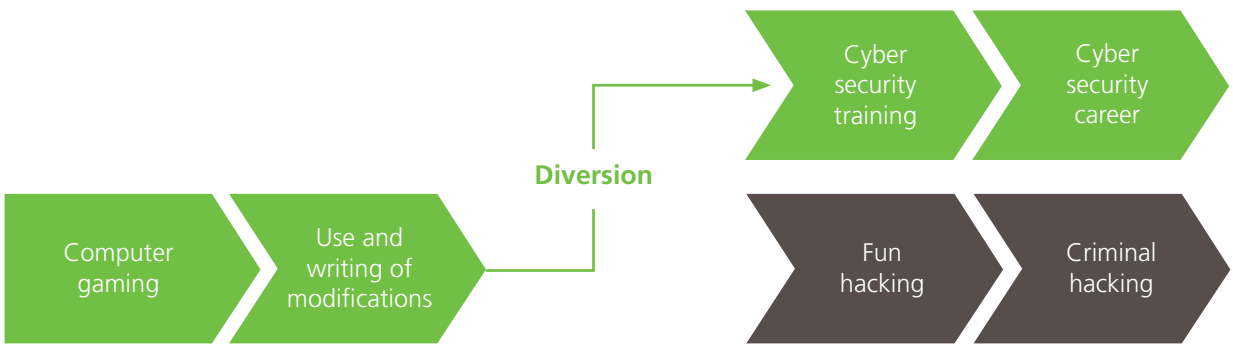
As well as ensuring there are enough cyber security experts to perform technical roles, professionals in various other roles within Financial Services should receive training that equips them with a basic understanding of cyber security. This has already started, for example with the recent Payments UK Cyber Security Conference of cyber professionals. With many data breaches occurring as a result of human error, Government should continue to educate those who on a regular basis use systems that are seen as a target by hackers, such as 'Cyber Security for Procurement Professionals'[46] and 'Cyber Security for Legal and Accountancy Professionals'[47]. Courses such as these provide a foundation for industry and Government to collaborate; with GCHQ, the Department for Business, Innovation and Skills, and the Chartered Institute of Procurement and Supply inputting on the former, and the Law Society, Institute of Chartered Accountants in England and Wales, and Government working together on the latter.

Just having the right courses and apprenticeships in place is not sufficient as firms need to also make sure that the right talent participates in them. Identifying and attracting the right calibre of staff is critical, and innovative initiatives by both Government and industry are required, such as the Cyber Security Challenge UK which involves national competitions and learning programmes looking to inspire talented individuals towards cyber security professions[48]. Likewise, GCHQ are looking to incentivise participation in extra-curricular activities by paying students £250 a week to attend their Cyber Summer Schools[49].

CREST is using a similar initiative to select its workforce, having identified that a typical pathway into criminal hacking originates through computer gaming, so they look to identify talent early that is heading in the direction of hacking and diverting it away towards cyber security. They offer ~20 graduate jobs per year in cyber for which candidates are entered into a hacking game online that is run for 4 months. Normally about 400 people register and play the game, with contestants gradually dropping out of the competition until CREST are left with the final 40 whom they know have the skills they need[50].

Figure 10

Alternative pathways for potential hackers



[45] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/275566/UKTI_Cyber_Security_Brochure.pdf
[46] http://www.cips.org/cybersecurity
[47] http://cpdcentre.lawsociety.org.uk/course/6707/cyber-security-for-legal-and-accountancy-professionals
[48] https://cybersecuritychallenge.org.uk/
[49] http://www.gchq.gov.uk/press_and_media/press_releases/Pages/GCHQ-Cyber-Schools-2016-applications-open.aspx
[50] Catching the Big Phish, Innovative Finance conference (15th June 2015)

6.0 ACTION PLAN

Our recommendations are given below. They fall into two categories:

6.1 RECOMMENDATIONS TO INDIVIDUAL FIRMS

- Make cyber risk a standing item on the Board or risk committee agenda
- Ensure cyber risk is a part of strategy, investment cases, acquisitions and appraisals
- Have a broad based team inputting to how cyber risk is managed
- Monitor cyber readiness against the ten-point cyber check list

Board Cyber Check-List

01 The main cyber threats for the firm have been identified and sized

02 There is an action plan to improve defence and response to these threats

03 Data assets are mapped and actions to secure them are clear

04 Supplier, customer, employee and infrastructure cyber risks are being managed

05 The plan includes independent testing against a recognised framework

06 The risk appetite statement provides control of cyber concentration risk

07 Insurance has been tested for its cyber coverage and counter-party risk

08 Preparations have been made to respond to a successful attack

09 Cyber insights are being shared and gained from peers

10 Regular Board review material is provided to confirm status on the above

6.2 RECOMMENDATIONS TO THE FINANCIAL AND RELATED PROFESSIONAL SERVICES SECTOR

- Set up an industry-wide Cyber Forum for major institutions to complement existing bodies
- Set an agenda for the Cyber Forum focused on systemic cyber risk reduction
- Make the case for cyber investment to be off-set against industry specific taxes
- Encourage the adoption of cyber standards in lending, underwriting and investment decision to promote cyber security in the wider economy

Cyber Forum Starting Agenda

01 Encourage information-sharing on cyber incidents

02 Encourage the adoption of best practice on cyber risk management

03 Engage in work on sector resilience to large-scale cyber attack

04 Engage in work on cyber risk aggregation

05 Support the development of a UK cyber security sector

APPENDIX A.
CYBER TASKFORCE MEMBERS AND CONTRIBUTORS

The Cyber Taskforce ("the Taskforce") was formed comprising an expert project team from Marsh Insurance and Oliver Wyman, the management consultancy.
The project team was supported by a Working Group of senior representatives from TheCityUK's leading corporate members with further input provided by a Steering Group of cross-industry practitioners. The review was conducted from October 2015 to March 2016.

1. Steering Committee

The Steering Committee for the development of this report comprised the following members:

- Stephen Catlin, Chairman, XL Catlin
- Clare Francis, MD Global Corporates, LBG
- Martin Gilbert, CEO, Aberdeen Asset Management
- Jane Jenkins, Partner, Freshfields
- Sushil Saluja, Senior MD, Accenture
- Clare Woodman, COO, Morgan Stanley

2. Taskforce project team

The Taskforce for the publication of this report comprised the following members:

- Mark Weil, CEO, Marsh Ltd (Taskforce Chairman)
- Marcus Scott, COO, TheCityUK
- Sir Iain Lobban, former director GCHQ
- Melissa Kelly, Chief of Staff, Marsh Ltd
- Matthew Wallace, Consultant, Oliver Wyman

3. Interviewees and contributors

To supplement our research, the Taskforce has spoken with a number of interviewees from a range of industries, and plan to continue this into January 2016.

- Vivienne Artz, Legal Managing Director Citigroup and Chair of IRSG, and Marisa Plowden, Legal Director, Citigroup
- Nick Beecroft, Manager of Emerging Risk and Research, Lloyd's of London
- Peter Church, Counsel PSL, Linklaters
- Rajesh De, Partner at Mayer Brown (head of Cybersecurity and Data Privacy practice)
- Richard Fenning, CEO, Control Risks
- Andrew Gracie, Executive Director for Resolution at the Bank of England; responsible for operational resilience of the financial sector, including cyber risk
- Jane Jenkins, Partner, Freshfields
- Rohini Kumar, Assistant Director, Financial Services & Education Sectors, Cyber Security Exports, UKTI
- Adrian Leppard, former Commissioner of the City of London Police, and Director, Templar Executives
- Alastair MacWilson, cyber security expert, senior adviser on digital risk and cyber, Parker Fitzgerald
- Craig Rice, Director of Security, Payments UK
- Ben de la Salle, Head of IT Security and Risk, Old Mutual Wealth
- John Unsworth, Deputy National Coordinator for Economic Crime, City of London Police
- Phil Westgarth, Information Security Manager, VocaLink, and Chair of Finance Strategy Co-ordination Group
- Jonathan Luff, Co-Founder, CyLon
- Nigel Wilson, Group CEO, Legal & General
- Bob Wigley, Chairman, NetOTC

APPENDIX B.
CYBER-RELATED BODIES GLOSSARYS

Centre for the Protection of National Infrastructure (CPNI): protects national security by enacting security measures or protocols to deter, detect or minimise the consequences of an attack.

Cross Market Operational Resilience Group (CMORG): Bank of England's coordination body for response to particular types of cyber attacks.

Government Communications Headquarters (GCHQ): security and intelligence organisation tasked by UK government to protect the country from potential threats that include cyber.

National Cyber Centre (NCC): dedicated "cyber force" to be created in Britain for handling cyber incidents, based at GCHQ.

National Security Council (NSC): main forum for collective discussion of national security objectives, chaired by the UK Prime Minister.

Office of Cyber Security and Information Assurance (OCSIA): determines priorities in relation to a secure cyberspace, working with Cabinet Office ministers and the National Security Council to coordinate the cyber security programme for the government.

UK National Computer Emergency Response Team (CERT-UK): manages cyber security incidents, supports critical national infrastructure, promotes cyber awareness and provides an international point of contact for co-ordination and collaboration between national CERTs.

Finance Strategy and Coordination Group (FSCG): an affiliation of Finance Services groups addressing the defence of information systems and networks against cyber threats, as well as engaging CMORG to promote collaboration and coordination of cyber security.

European Union Agency for Network and Information Security (ENISA): provides EU member states and other actors with the platform to exchange information, best practices and knowledge in the field of Information Security.

Financial Services Information Sharing and Analysis Centre (FS-ISAC): a global organisation providing cyber and physical threat intelligence analysis and sharing for its Financial Services members.

Global Cyber Alliance (GCA): a not-for-profit organisation dedicated to challenging the cyber threat and bringing the criminals to justice through international cooperation.

UK Trade & Investment (UKTI): government department working with businesses based in the UK to promote their international success.

Cyber Growth Partnership (CGP): group of UK industry, government and academia representatives ensuring that UK firms are able to grow, thrive and innovate, in order to become world leaders in cyber security.

National Cyber Crime Unit (NCCU): leads UK's response to cyber crime, providing specialist capabilities to partners (including crime unit, industry, government and international law enforcement) and coordinating the response to the most serious threats.

BIBLIOGRAPHY

1. Advisen database (2015)
2. Andrew G Haldane, speech on "The $100 billion question" (2010) - http://www.bis.org/review/r100406d.pdf
3. Australian Government, Top four mitigation strategies to protect your ICT system (2012) - http://www.asd.gov.au/publications/protect/Top_4_Mitigations.pdf?&verNov12
4. Bank of England, CBEST Vulnerability Testing Framework Launch (2015) - http://www.bankofengland.co.uk/financialstability/fsc/pages/cbest.aspx
5. Bank of England, Financial Stability Report (2015) - http://www.bankofengland.co.uk/publications/Documents/fsr/2015/dec.pdf
6. BBC, "Hack attack causes 'massive damage' at steel works" (2014) - http://www.bbc.com/news/technology-30575104
7. Catching the Big Phish, Innovative Finance conference (2015)
8. Centre for Strategic and International Studies, Net Losses: Estimating the Global Cost of Cyber Crime (2014) - http://csis.org/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf
9. CERT-UK, Annual Report Apr 2014 – Mar 2015 (2015) - https://www.cert.gov.uk/wp- content/uploads/2015/05/Annual-Report-including-4th-Quarter-FINAL.pdf
10. CERT-UK, Cyber-security Information Sharing Partnership (2015) - https://www.cert.gov.uk/cisp/
11. CERT-UK, CERT-UK Weekly Update (2016) - https://www.cert.gov.uk/wp- content/uploads/2016/01/20160114-Weekly-Update.pdf
12. Chartered Institute of Procurement & Supply, Cyber Security ELearning (2015) - http://www.cips.org/cybersecurity
13. CISCO, CISCO Visual Networking Index (2015) - http://www.cisco.com/c/en/us/solutions/service- provider/visual-networking-index-vni/index.html
14. City of London Police, "Fraud and Cyber-Crime: What's being done?" (2015) - https://www.cityoflondon.police.uk/news-and-appeals/Pages/Adrian-Leppard-Fraud-and-Cyber-crime.aspx
15. Clifford Chance, Cyber Security – Legal and Regulatory Considerations (2015) - http://www.cliffordchance.com/briefings/2015/06/cyber_security_legalandregulator.html
16. Clifford Chance, Safe Harbor declared invalid – what it means for your business (2015) - http://www.cliffordchance.com/briefings/2015/10/safe_harbor_declaredinvalidwhatitmeansfo.html
17. Council on Foreign Relations, "Cleaning Up U.S. Cyberspace" (2015) - http://www.cfr.org/internet- policy/cleaning-up-us-cyberspace/p37333
18. CPNI, Critical Security Controls guidance (2012) http://www.cpni.gov.uk/advice/cyber/Critical-controls/
19. CREST, Member Companies (2015) - http://crest-approved.org/crest-member-companies/member-companies/index.html
20. Cyber Growth Partnership, Registered UK Companies Directory (2016) - https://www.cgp.uk.net/#/directory
21. CyberGym (2015) - https://www.cybergymeurope.com/
22. Cyber Security Challenge UK (2015) - https://cybersecuritychallenge.org.uk/
23. Cyber Security Index, Summary reports on Index of Cyber Security (2012-2015) - http://www.cybersecurityindex.org/
24. Cyence database (2015)
25. Defense News, "Israel Claims $3B in Cyber Exports; 2nd Only to US" (2014) - http://archive.defensenews.com/article/20140620/DEFREG04/306200018/Israel-Claims-3B-Cyber-Exports-2nd-Only-US
26. ENISA, Incentives and barriers of the cyber insurance market in Europe (2012) - https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/incentives-and-barriers-of-the-cyber-insurance-market-in-europe/at_download/fullReport

27vEurex, High-frequency trading – a discussion of relevant issues (2013) - http://www.eurexchange.com/blob/exchange-en/4038-4046/426058/2/data/presentation_hft_media_workshop_chi_nyc_en.pdf

28. European Banking Authority, Consultation paper for Article 107 (3) of Directive 2013/36/EU (2014) - https://www.eba.europa.eu/documents/10180/748829/EBA-CP-2014-14+%28CP+on+draft+SREP+Guidelines%29.pdf
29. European Commission, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (2013) - http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf
30. European Commission, Press release: "Commission welcomes agreement to make EU online environment more secure" (2015) - http://europa.eu/rapid/press-release_IP-15-6270_en.htm

31. Export Virginia, Cyber Security Export Market: Saudi Arabia (2014) - http://exportvirginia.org/wp-content/uploads/2014/02/Saudi-Arabia.pdf
32. Finance Strategy & Co-ordination Group, UK Finance Sector security collaboration groups and their national and international links (2015)
33. Financial Times, Transcript: FT City Network debates cyber crime (2015) - http://www.ft.com/cms/s/0/b1e350c4-a27b-11e5-bc70-7ff6d4fd203a.html#axzz3vtqn5rvC
34. Forbes, "Greek Bank Closure Cost Economy €3 Billion, Banks Reopen Monday" (2015) - http://www.forbes.com/sites/timworstall/2015/07/18/greek-bank-closure-cost-economy-e3-billion-banks- reopen-monday/
35. Gartner, Information Security, Worldwide, 2Q15 Update (2015) - http://www.gartner.com/newsroom/id/3135617
36. GCHQ, Press release: "£6.5 million CyberInvest scheme to boost world-class UK cyber security research" (2015) - http://www.gchq.gov.uk/press_and_media/press_releases/Pages/cyberinvest-boosts- uk-cyber-research.aspx
37. GCHQ, Press release: "Applications open for GCHQ's Cyber Summer Schools" (2016) - http://www.gchq.gov.uk/press_and_media/press_releases/Pages/GCHQ-Cyber-Schools-2016-applications-open.aspx
38. GCHQ, Press release: "Cyber First scheme launched to develop the UK's next generation of cyber security experts" (2015) - http://www.gchq.gov.uk/press_and_media/news_and_features/Pages/launch-of-Cyber-First-scheme.aspx
39. HM Government, Cyber Essentials scheme (2014) - https://www.gov.uk/government/publications/cyber- essentials-scheme-overview
40. HM Government, 2015 Information Security Breaches Survey (2015) - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/432412/bis-15-302-information_security_breaches_survey_2015-full-report.pdf
41. HM Government, 10 steps to cyber security (2015) - https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary
42. HM Government, The UK cyber security strategy (2011) - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf
43. HM Government, The UK's Strategy for Countering International Terrorism (2010) - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228907/7833.pdf
44. HM Government, Cyber Security: The UK's approach to exports (2014) - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/275566/UKTI_Cyber_Security_Brochure.pdf
45. HM Government, UK cyber security: the role of insurance (2015) - https://www.gov.uk/government/publications/uk-cyber-security-the-role-of-insurance
46. HM Government, UK defence and security export figures 2014 (2015) - https://www.gov.uk/government/statistics/uk-defence-and-security-export-figures-2014
47. IBM, 2014 Cyber Security Intelligence Index (2014) - http://www-03.ibm.com/security/services/2014-cyber-security-intelligence-index-infographic/index.html
48. IMF, Greece: An update of IMF staff's preliminary public debt sustainability analysis (2015) - http://www.imf.org/external/pubs/ft/scr/2015/cr15186.pdf
49. Independent, "Two charts that show what's threatening internet security more than a cyber attack" (2015) - http://www.independent.co.uk/news/business/news/two-charts-that-show-the-one-thing- threatening-personal-data-online-more-than-cyber-attack-a6712391.html
50. Institute of Risk Management, Cyber risk and risk management (2015) - https://www.theirm.org/knowledge-and-resources/thought-leadership/cyber-risk/
51. Investment Industry Regulatory Organization of Canada, Cyber Incident Management Planning Guide (2015) - http://www.iiroc.ca/industry/Documents/CyberIncidentManagementPlanningGuide_en.pdf
52. IT Governance, "Three quarters of companies risk serious security breach from ex-employees" (2015) - http://www.itgovernance.co.uk/blog/three-quarters-of-companies-risk-serious-security-breach-from-ex-employees/
53. Kaspersky, Future Risks: Be Prepared (2014) - http://media.kaspersky.com/en/business-security/APT-Report.pdf
54. Kaspersky, "The Threat Within: 3 Out Of 4 Companies Affected By Internal Information Security Incidents" (2015) - http://www.kaspersky.com/about/news/product/2015/The-Threat-Within-3-Out-Of-4-Companies-Affected-By-Internal-Information-Security-Incidents
55. Lloyds, Market bulletin: "Cyber-attack: managing catastrophe-risk and exposures" - https://www.lloyds.com/~/media/files/the%20market/communications/market%20bulletins/2015/11/y4938.pdf

56. London First, "Discussion at London First Roundtable with The Rt Hon Francis Maude MP" (2013) - http://londonfirst.co.uk/wp-content/uploads/2013/11/Roundtable-with-Rt-Hon-Francis-Maude-MP- National-Cyber-Security-Programme-Background.docx
57. Macquarie Research, Security: Cyber Insurance (2015)
58. MarketsandMarkets, Cyber Security Market by Solution – Global Forecast to 2020 (2015) - http://www.marketsandmarkets.com/PressReleases/cyber-security.asp
59. Marsh, UK 2015 Cyber Risk Survey Report (2015) - https://www.marsh.com/uk/insights/research/uk-2015-cyber-risk-survey-report.html
60. Marsh, European 2015 Cyber Risk Survey Report (2015) - http://uk.marsh.com/Portals/18/Documents/European%202015%20Cyber%20Risk%20Survey%20Report-10-2015.pdf
61. Masterpass (2015) - https://masterpass.com/
62. Matthew Gould, Director of Cyber Security and Information Assurance at the Cabinet Office, speaking at Marsh's 8th Annual Client Conference on the (2015)
63. Nato, The History of Cyber Attacks – a timeline (2013) - (http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm
64. New York Times, "Cyberattack at JPMorgan Chase Also Hit Website of Bank's Corporate Race" (2014) - http://dealbook.nytimes.com/2014/10/15/cyberattack-at-jpmorgan-chase-also-hit-website-of-banks-corporate-race/?_r=1
65. NIST, Press release: NIST Releases Cybersecurity Framework Version 1.0 (2014) - http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm
66. ONS, "Improving crime statistics in England and Wales" (2015) - http://www.ons.gov.uk/ons/rel/crime-stats/crime-statistics/year-ending-june-2015/sty-fraud.html
67. Parliament, Protecting Europe against large-scale cyber-attacks (2010) - http://www.publications.parliament.uk/pa/ld200910/ldselect/ldeucom/68/6805.htm#a3
68. Payments Council, Cyber Threat Intelligence whitepaper (2014)
69. PivotPoint database (2015)
70. RBC Capital Markets, A deeper look at key cyber-security trends (2015)
71. Telegraph, "Bank of England adviser: 'Everyone should have two bank accounts in case of cyber attack'" (2015) - http://www.telegraph.co.uk/finance/personalfinance/bank-accounts/12028576/Bank-of- England-adviser-Everyone-should-have-two-bank-accounts-in-case-of-cyber-attack.html
72. The Law Society, Cyber Security for Legal and Accountancy Professionals (2015) - http://cpdcentre.lawsociety.org.uk/course/6707/cyber-security-for-legal-and-accountancy-professionals
73. The Rt Hon George Osborne MP, speech on Cyber Security at GCHQ (2015) - https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security
74. US-CERT, Information sharing specifications for cybersecurity - https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity
75. US District Court for the Central District of California, Columbia Casualty Company v. Cottage Health System (2015) - https://securityledger.com/wp-content/uploads/2015/05/Columbia-v-Cottage.pdf
76. Veritas, The Databerg Report (2015) - http://info.veritas.com/databerg_report
77. Verizon, PCI Compliance Report (2015) - http://www.verizonenterprise.com/resources/report/rp_pci-report-2015_en_xg.pdf
78. Visa, All you need to know about Tokenisation (2015) - https://usa.visa.com/dam/VCOM/Media%20Kits/PDF/visa-security-tokenization-infographic.pdf
79. Wall Street Journal, "Merger That Came to Aid of Knight Capital Struggles" (2015) - http://www.wsj.com/articles/merger-that-came-to-aid-of-knight-capital-struggles-1427669088
80. Wall Street Journal, "Target Now Says 70 Million People Hit in Data Breach" - http://www.wsj.com/articles/SB10001424052702303754404579312232546392464
81. Water ISAC, 10 Basic Cybersecurity Measures (2015) - https://ics-cert.us-cert.gov/sites/default/files/documents/10_Basic_Cybersecurity_Measures-WaterISAC_June2015_S508C.pdf
82. Wells Fargo, Insurance 2016 Outlook (2016)
83. World Economic Forum, Global Risks Report 2016 (2016) - http://www3.weforum.org/docs/GRR/WEF_GRR16.pdf

ADDITIONAL READING

1. CBEST - http://www.bankofengland.co.uk/financialstability/fsc/pages/cbest.aspx
2. CERT-UK - https://www.cert.gov.uk/
3. Cyber Essentials - https://www.gov.uk/government/publications/cyber-essentials-scheme-overview
4. European Commission - https://ec.europa.eu/digital-agenda/en/cybersecurity
5. FS-ISAC - https://www.fsisac.com/
6. GCHQ - http://www.gchq.gov.uk/pages/homepage.aspx
7. HM Government cyber security policies - https://www.gov.uk/government/policies/cyber-security
8. MMC Cyber Risk Handbook 2015 - https://www.marsh.com/us/insights/cyber-risk- handbook-2015.html
9. NIST - http://www.nist.gov/cyberframework/
10. UKTI - https://www.gov.uk/government/organisations/uk-trade-investment

Marsh is a global leader in insurance broking and risk management. Marsh helps clients succeed by defining, designing, and delivering innovative industry-specific solutions that help them effectively manage risk. Marsh's approximately 30,000 colleagues work together to serve clients in more than 130 countries. Marsh is a wholly owned subsidiary of Marsh & McLennan Companies (NYSE: MMC), a global professional services firm offering clients advice and solutions in the areas of risk, strategy, and people. With annual revenue of US$13 billion and approximately 60,000 colleagues worldwide, Marsh & McLennan Companies is also the parent company of Guy Carpenter, a leader in providing risk and reinsurance intermediary services; Mercer, a leader in talent, health, retirement, and investment consulting; and Oliver Wyman, a leader in management consulting. Follow Marsh on Twitter, @MarshGlobal; LinkedIn; Facebook; and YouTube.

1 Tower Place West, Tower Place, London EC3R 5BU
+44 20 7357 1000
Cyberandthecity@marsh.com

TheCityUK

TheCityUK, Salisbury House, Finsbury Circus, London EC2M 5QQ
www.thecityuk.com

For further information about this report, please contact:

Marcus Scott, Chief Operating Officer, TheCityUK
marcus.scott@thecityuk.com