Promoting UK Cyber Prosperity: Public-Private Cyber-Catastrophe Reinsurance

July 2015

A Long Finance report prepared by Z/Yen Group and co-sponsored by APM Group

Promoting UK Cyber Prosperity:
Public-Private Cyber-Catastrophe Reinsurance

July 2015

A Long Finance report prepared by Z/Yen Group
Co-sponsored by APM Group

Z/Yen Group Limited
90 Basinghall Street,
London EC2V 5AY
UK

+44 (20) 7562-9562 (telephone)
+44 (020) 7628-5751 (facsimile)
hub@zyen.com (email)
www.zyen.com (web)

FOREWORD

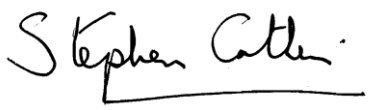
Cyber-risk has the potential to be the biggest, most systemic risk I have encountered in my insurance career. It is big because the information and telecommunications revolution of the past half-century means that computers are now used for practically everything. It is systemic because the very nature of telecommunications means everything is now connected with everything else. As we move to the fabled 'Internet of Things' – i.e. everyday objects sending, receiving, and processing data autonomously – the systemic risk grows exponentially.

The systemic risk is also financial. We can easily imagine scenarios where a major computer outage – whether due to cyber-terrorism, power failure or a super solar storm – could lead to massive property damage and business interruption. Our potential nightmares range from destruction of the contents of all freezers, to massive pile-ups of autonomous vehicles, to interference with medical devices implanted in people.

Insurance has had a major role to play in managing many of society's previous 'big' risks; fire, flood, theft, employer's liability, automotive, shipping, and aviation come easily to mind. However, the global and systemic nature of cyber-risk means that insurers are restricted in their ability to work with society to manage this risk. Our regulators expect us, quite rightly, to manage our balance sheets. However, our balance sheets are not large enough to pay for a true cyber-catastrophe. This is where a fresh approach to reinsurance will help insurers enter the market more rapidly and usefully.

This report considers the systemic nature of cyber-risk and the potential cyber-catastrophes ahead. The report recommends a UK Public-Private Cyber-Catastrophe Reinsurance scheme to begin addressing this systemic risk and to help insurers take proactive steps to tackle this problem for the benefit of society. Our future prosperity depends on our cyber-economy. Equally, our future prosperity depends on the intelligent management of physical and financial cyber-risk. A Public-Private Cyber-Catastrophe Reinsurance scheme would help accelerate the growth of cyber-insurance to help our cyber-economy flourish.

We as insurers and reinsurers should never be afraid of taking real risk on our balance sheets, but that risk must be containable if we are to honour the promise to pay. This is a real opportunity for our industry to add value to society alongside government support for the benefit of the whole.



Stephen Catlin
Executive Deputy Chairman, XL Catlin

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

The UK's prosperity, present and future, depends on information & communications technology (ICT) in our increasingly 'cyber' world. This report takes that as given. However, our dependence on cyber grows each year, and our cyber is vulnerable. Malicious people can harm society both through ICT and by attacking society's ICT. Our dependence also exposes us more to natural risks such as a super solar flare. This report explores how a public-private cyber-catastrophe reinsurance scheme could better secure ICT-based prosperity.

Cyber-risk is real. If newspaper coverage were a measure, cyber attacks are growing enormously according to headlines. Though there is specific case information, authoritative numbers about the extent of attacks and damages are more problematic. Crimes such as 'cyber extortion', an attack or threat accompanied by a demand for money, discourage people from reporting. Victims of attacks may not wish to publicise attacks, thus leading to under-reporting. There is no requirement to report incidents or single authority to whom to report. Many people are unaware of the scale of daily hacking attempts on their own computer systems, let alone on supporting infrastructure and utilities.

Knowledge about attackers is limited. Anecdotally, lone teenagers, organised crime gangs, rogue states, and even national security bodies commonly engage in cyber attacks. It is extremely difficult to ascertain the cause, effect, and intent of a cyber attack with certainty, even more difficult where state involvement is suspected. Is a criminal gang working in Central Asia with state complicity to extort money from a UK bank simple criminality, or warfare, or terrorism?

Defence by the victims is also problematic. Traditional risk management requires reasonable estimates of impact and likelihood. The impact can range from virus inconvenience to intellectual property theft to complete business shutdown to economic meltdown. Notable viruses such as the Neverquest Trojan have inconvenienced millions of people by stealing their online bank account access details. Companies have experienced significant theft of property, a recent example being Sony Pictures Entertainment in 2014. Entire networks and related infrastructure have been shut down with Stuxnet. As yet, there has been no national economic meltdown though, to take one example, the country of Estonia sustained enormous and damaging cyber attacks during 2007. An organisation could pay an infinite amount for protection without guarantees of safety, rendering cost/benefit analysis impotent.

With the increasing computerisation and networking of society, there are ever more ways to attack systems with malicious intent. Inter-connectivity increases the number of systemic risk points, such as common pieces of software replicated everywhere or concentrated communication nodes whose downfall would affect millions. Inter-connectivity increases the potential impact of cyber attacks, and thus their attractiveness in offence and complexity in defence. It is little surprise that many businesses take a 'no fault in numbers' approach. If their systems are successfully attacked, as long as they cannot be blamed for being much worse than others, it does not matter.

Insurance is a pooling mechanism that helps people transfer risks. Insurance has helped the UK in the past transfer risks such as fires, workplace injuries, or automotive thefts. The current cyber insurance market is limited. 'Cyber insurance' is a broad term covering a variety of policies. Some policies cover legal and administrative costs in the case of data breaches, when perhaps millions of customers need to be notified. Other policies provide protection advice and then provide more consultancy in the event of a claim. Some cyber-risks are covered in some existing policies, though the wordings vary and the coverage is, at best, patchy. The commonly used Lloyd's Market Association Cyber Attack Exclusion

(CL380) and Non-Marine Association's Electronic Data Exclusion NMA2914 in insurance policies open gaping holes in cyber insurance coverage. Insurance for core risks, viz. property damage, business interruption, and third party liability, is difficult to obtain at a reasonable scale, such as that required by a financial institution or online retailer. Another risk, damages for the theft of intellectual property, is probably uninsurable.

Aggregation can occur when one cyber event triggers multiple claims under different policies (for example reputational risk, Property Damage, Professional Indemnity, and Directors Errors & Omissions), one cyber event triggers multiple claims by multiple clients under different policies, or one cyber event unveils multiple past attacks triggering multiple claims across multiple underwriters. Stiff regulatory capital requirements impede, correctly, insurers taking on too much exposure in the event such aggregation overwhelms them, but stiff capital requirements in the event of a cyber-catastrophe impede the ability of insurers to write 'normal' property damage, business interruption, and third party liability cover that includes cyber.

A report by HM Government and Marsh, "UK Cyber Security: The Role Of Insurance In Managing And Mitigating The Risk" (March 2015) reviewed cyber cover noting "the combination of a higher absolute price and lower price differentiation suggests that cyber is early in its development". Michel Liès of Swiss Re describes cyber as "borderline insurable" (Liès, 2015: 1). One of the biggest problems is the chasm between retail and wholesale insurance in a nascent market, a liquidity issue. Insurers find writing cyber insurance difficult without reinsurers, but reinsurers need significant scale before the pooling effects make such reinsurance possible.

In the face of rapidly growing cyber-risk, the tools of insurance, i.e. risk management and shared learning, need to be rapidly grown and deployed. To increase the rate of learning, society needs to increase the rate of cyber cover. If society wishes to bring insurance to bear on helping to manage cyber-risk, then cyber-catastrophe reinsurance needs to be available for property damage, business interruption, and third party liabilities in order to remove blockages to rapid take-up of cyber insurance by businesses.

This report outlines a public-private cyber-catastrophe reinsurance scheme that would help insurers insure themselves to insure others. The scheme would provide cover to a group of insurers above a catastrophic loss threshold (to be defined by government and the industry), excluding intellectual property theft and reputational risks. The benefits of such a scheme are that it provides a way to help industry, insurers, and government pull together to manage this huge risk on UK plc's balance sheet by supporting more objective pricing of risk through premiums. The scheme does so by encouraging appropriate information sharing, standards, and best practice alongside insurance-based incentives for investment in protection. The key points of such a scheme are that:

- the scheme should provide more standardised wordings linking cyber-catastrophe to the policies members write, and more standardised data collection for analytical purposes;
- the scheme should promote the use and evolution through learning of ICT security and risk management standards such as Cyber Essentials, ISO 27000, NIST, or CESG's 10 Steps;
- insurance regulators should strongly encourage membership by insurers providing cyber cover;
- members should jointly seek reinsurance for a cyber-catastrophe, including consideration of cyber-catastrophe linked securities;
- government should facilitate, but not underwrite, the scheme's reinsurance – government oversight could help the issuance of cyber-catastrophe linked bonds;
- government and regulators should strongly encourage cyber insurance for essential services and critical national infrastructure including financial services, and incorporate

cyber insurance in government procurement processes, e.g. requirement to purchase if unable to show appropriate management or retentions.

A public-private cyber-catastrophe reinsurance scheme could be a new scheme, or an extension to the existing Pool Re for terrorism. Extending Pool Re would perhaps be easiest as there is already a mutual structure; potentially some seed funds for development; a risk assessment capability; and a track record of successful funding and operations. More work needs to be done by members of such a scheme on the likely thresholds for reinsurance. It would, of course, be easier to motivate people to action after a black swan event, but under the umbrella of an existing Pool Re action could start immediately.

A public-private cyber-catastrophe reinsurance scheme would not only improve UK cyber resilience but also improve UK competitiveness as an attractive economy to locate cyber business, and a place to source cyber-risk and security experts who have proven their financial, as well as technical, prowess.

2. INTRODUCTION

2.1 Background

Cyber attacks are becoming more common, sophisticated, and damaging. The variety of attacks is increasing. Losses include (from Willis, 2014):

First Party Cyber Losses

- network interruption due to:
  - computer crime;
  - employee sabotage;
  - operational errors and administrative mistakes;
  - cyber terrorism;
- restoration, recollection, recreation of digital assets due to:
  - computer crime;
  - employee sabotage;
  - operational errors and administrative mistakes;
  - accidental damage to hardware;
- cyber extortion.

Data Privacy And Security Third Party Losses

- breach of sensitive third party information;
- data breach caused by a third party outsourcer;
- corruption of third party data by malicious code;
- distributed denial of service or malicious code delivered via your network;
- corruption or deletion of third party data;
- lost/stolen laptop or hardware containing sensitive third party data;
- data breach due to a security breach;
- intellectual property infringement, plagiarism and defamation.

Data Privacy And Security First Party Losses

- data protection fines and penalties;
- data protection investigation and defence expenses;
- public relations costs;
- data protection legal expenses;
- data breach notification expenses;
- credit/identity theft monitoring expenses.

Aspects that illustrate the complex nature of cyber-risk include oversight of attack. Cyber attacks often go undetected for a while. When detected, many attacks are not reported by victims or misreported as IT malfunctions in order to protect organisational reputation. The perpetrators of an attack are frequently difficult to trace, which in turn makes attribution complex. Motives behind cyber attacks, whether political or economic, often overlap. State-involvement is sometimes suspected but never publicly acknowledged.

From a risk mitigation perspective, the cyber insurance market is still in its infancy. Standards guiding cyber vulnerability assessments and management are only starting to emerge. In March 2015, Marsh and HM Government published a report exploring how the insurance industry might help make UK companies more resilient to cyber threat. Recognising the potential for cyber attacks to cause costly and public disruption, the report also noted the lack of awareness on cyber insurance products and the low level of cyber insurance cover with only 2% of large firms having explicit cyber cover (Marsh & Cabinet Office, 2015).

This report is the outcome of a Long Finance study carried out by Z/Yen Group from April to July 2015 and co-sponsored by APM Group (more information). The study explored the nature of cyber-risk and the role of cyber insurance and reinsurance as a risk mitigation tool. The study concentrated on cyber-catastrophe events, cyber attacks that could seriously affect the UK economy. The study sought to:

- understand how cyber-catastrophe reinsurance might help mitigate general cyber risk;
- establish some evidence of the appetite for such reinsurance;
- examine how the insurance industry and UK government might create a cyber-catastrophe reinsurance scheme without public subsidy.

2.2 Approach & methodology

Following desk research, Z/Yen Group sought to engage experts and professionals working with:

- insurance brokers and underwriters both general and working specifically on specialty casualty, terrorism and cyber-risks;
- reinsurance companies;
- existing public-private reinsurance schemes such as Pool Re;
- ICT companies;
- cyber security companies and providers of cyber resilience solutions;
- major financial services firms such as exchanges, banks, and payment systems;
- law and accountancy firms;
- UK regulators and government departments.

Over 80 semi-structured interviews were carried out between May and July 2015, of which over half were with professionals working in insurance and reinsurance. The interviews explored cyber-catastrophe as part of a broader cyber-risk environment, the state of the cyber insurance market, the insurance's industry appetite for cyber reinsurance, the scale of potential losses and benefits, and how a public-private cyber-catastrophe reinsurance scheme might work.

A webinar presented preliminary findings for wider discussion on 24 June 2015 (more information). 20 people attended the webinar including representatives of local and national government, the insurance industry, ICT firms and financial services. The audience was primarily UK-based though interested parties in the USA later accessed the recording.

The Centre for the Study of Financial Innovation (CSFI) kindly hosted a round-table on 30 June 2015 to discuss cyber insurance. Dr Andrew Hilton chaired the event. Speakers included Michael Mainelli (Z/Yen Group's executive chairman and co-author of this report), Julian Enoizi (Chairman of Pool Re), Russell Kennedy (Brit Insurance), and Mike St John Green (cyber security expert). Over 70 people attended the event in the City of London.

2.3 Report outline & acknowledgements

This report comprises six chapters. Besides the executive summary (Chapter 1) and this introduction to the report (Chapter 2):

- Chapter 3 explores the nature of cyber-risk, analyses recent evidence of cyber attacks and seeks to define what catastrophic cyber-risk might look like;
- Chapter 4 explores how cyber-risk can be mitigated through insurance and provides an overview of the current state of the cyber insurance market in the UK and globally;
- Chapter 5 explores the feasibility and appetite for a public-private cyber-catastrophe reinsurance scheme and outlines possible approaches;
- Chapter 6 provides recommendations for future developments.

This report includes five appendices:

- Appendix 1 provides an overview of selected cyber attacks - the evidence illustrates how difficult it can be to categorise cyber attacks and to ascertain state involvement;
- Appendix 2 compares terrorism risk insurance programmes in selected countries (Australia, France, Germany, UK and USA) based on their purpose and insurance cover, including how cyber-risk might be included or excluded from the insurance cover;
- Appendix 3 contains the interview template for insurers;
- Appendix 4 lists the affiliations of people who have kindly contributed to this project;
- Appendix 5 provides the bibliography, with much of the reference material available online.

This report was prepared by Michael Mainelli, Chiara von Gunten and Mark Duff of Z/Yen. We are very grateful to APM Group for their support and we would like to thank all the participants who agreed to semi-structured interviews and contributed to discussions during events. We received enthusiastic participation from everyone on this project, and it was a pleasure to meet so many people interested in helping to mitigate cyber risks.

3. UNDERSTANDING CYBER-RISK

Understanding the nature and evidence of cyber-risk is critical in order to assess how a cyber-catastrophe could adversely affect the UK economy and its cyber prosperity. On 16 January 2015, the then UK Business Secretary Vince Cable said "The UK has a world-leading digital economy, growing three times as fast as our overall economy and employing over a million people. Our businesses earn £1 in every £5 from the internet, so it's vital that we work with them to combat online crime, and make sure large and small firms alike are protected."

This chapter has three parts. Section 3.1 defines cyber-risk; explores the means, actors and motives behind cyber attacks, and provides estimates of the cost of cyber breach to the economy. Section 3.2 provides an overview of the evidence of recent attacks to illustrate how difficult it can be to categorise cyber events according to their cause, effect and intent. Section 3.3 starts to define what could constitute a cyber-catastrophe whose resulting losses would threaten the UK's economic stability and security.

3.1 Nature of the risk

A cyber threat is the risk of a breach of "the confidentiality, integrity and accessibility of an entity's online or computer presence or networks and the information contained within" (Tendulkar, 2013). Associated risks and impacts can be due to human or system errors but also to deliberate attempts to cause harm. As reliance on ICT and the Internet increases and systems become more interconnected and interdependent, so does the potential for vulnerabilities in ICT (and related infrastructure and processes) to be exploited for malicious purposes leading to adverse consequences.

Cyber-risk is increasingly perceived as a global risk to society and the economy. Anyone using computers connected to networks is potentially exposed to cyber-risk. This is particularly true for organisations that store or outsource the storage of sensitive data (including personal records) and/or are reliant on the Internet, digital information, web pages, networks and computers. Revelations about cyber attacks, including data theft and cyber espionage in the media have increased in frequency. 'Cyber attacks' rated 10th in the top 10 global risks in terms of likelihood and 'critical information infrastructure breakdown', and 7th in the top 10 global risks in terms of impact according to WEF's Global Risk Report 2015 (World Economic Forum, 2015). Insurance, banking and microfinance professionals across 50 countries also rated cyber-risk as the fourth global risk in the latest edition of a bi-annual survey (CSFI, 2015).

3.1.1 Types of cyber attacks, actors and motives

Cyber attacks aim to exploit vulnerabilities in systems. They can be divided into targeted and untargeted attacks (from GCHQ & Cert-UK, 2015).
Untargeted cyber attacks include:

- *phishing* – sending emails to large number of people asking for sensitive information (e.g. bank details) or encouraging them to visit a fake website;
- *water holing* - setting up a fake website or compromising a legitimate one in order to exploit visiting users;
- *ransomware* - disseminating disk encrypting extortion malware;
- *scanning* - attacking wide swathes of the internet at random.

Targeted cyber attacks include:

- *spear-phishing* - sending emails to targeted individuals that could contain an attachment with malicious software, or a link that downloads malicious software;

- *deploying a botnet* - executing a distributed denial of service (DDoS) attack which aims to flood an information gateway with data exceeding its bandwidth thus rendering the gateway or website inaccessible;
- *subverting the supply chain* - attacking equipment or software being delivered to organisations.

Cyber attacks can involve traditional crime typologies such as fraud or forgery committed through networks and information access, as well as new typologies fostered by the unique opportunities presented by the Internet. Common cyber crimes include the publication of harmful, illegal or false information via electronic media; the theft, destruction or manipulation of data; identity theft; monetary theft; intellectual property theft; disruption of IT services and networks or of other connected equipment and infrastructure (Tendulkar, 2013).

While the literature argues that cyber attacks can be distinguished based on frequency, actors, scale and motive (see Box 1), the reality suggests that it can take years to spot an attack and even more to identify the perpetrator, understand the motives and assess the full extent of the damage (Tendulkar, 2013).

Cyber attacks can come from a range of actors, including state-sponsored actors, e.g. foreign intelligence services; terrorist groups; organised crime networks and organisations; private enterprises; activists (e.g. Anonymous); opportunistic cyber criminals; current/former employees; and lone hackers. Motives behind a cyber attack can be of an economic, political, social or ideological nature and tend to overlap. Examples of motives include: panic and chaos; disruption; to harm a rival group, company or country; financial gain; expressing a message; ideological reasons; and publicity (see for example Detica & Cabinet Office, 2011; Marsh & Cabinet Office, 2015; CRO Forum, 2014; Tendulkar, 2013).

Cyber threats are not as easily identifiable as physical threats. First, while it may be relatively easy to spot the build up of physical capabilities, cyber-crime capabilities can be more easily hidden. Second, most physical threats have an immediate, observable outcome and are relatively easy to trace. The globalised nature of the Internet makes attacks difficult to trace. Cyber attacks can be launched from anywhere in the world and be routed through servers of third-party countries. As an example, the ‘Equation’ group, a highly sophisticated threat actor that has engaged in multiple computer network exploitation operations dating back to 2001 if not earlier, is thought to use infrastructure that includes more than 300 domains and over 100 servers across multiple countries (Kaspersky Lab, 2015).

Cyber capabilities are increasingly appealing to a range of actors including terrorist groups. In fact, compared to physical attacks, cyber attacks involve comparatively lower financial costs; the prospect of anonymity; a wider selection of available targets; the ability to conduct attacks remotely; and the potential for multiple casualties (Weimann, 2004). In addition, the threat of significant reprisal can be low.

Box 1 - Cyber-everything: crime, terrorism, hacktivism and warfare

Cyber attacks are said to differ depending on who causes them, their effect and their intent. Cyber-terrorism and cyber-warfare are increasingly being distinguished from other types of cyber crime on the grounds that the attacker's intent is primarily political (or social, religious or similar) rather than purely one of financial gain. The table below illustrates how such a distinction can be conceptualised based on frequency, the actors involved, the scale of the attack and the primary motive.

Figure 1 – Differences between cyber crime and cyber-terrorism/cyber-warfare

	Cyber crime	Cyber-terrorism and cyber-warfare
Frequency	Often re-occurring and common events	Usually highly isolated and unique incidents
Actors	Often a mix between individual and organised criminals with potentially some state involvement	Often solely instigated by state-sponsorship
Scale of the attack	Usually the scale of attack is not planned to be critically damaging to the UK economic infrastructure	Potential scale is often designed to cause maximum damage to UK infrastructure
Primary motive	Financial	Threaten UK socio-political infrastructure

[Source: Detica & Cabinet Office, 2011: 6]

Academia has long debated the concepts of cyber-terrorism, cyber-warfare and hacktivism. One definition of cyber-terrorism (possibly the most popular) is: "Cyberterrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives" (Denning, 2000:1). Cyber-terrorist attacks tend to be primarily political and target a specific country. Denning distinguishes between destruction and disruption, suggesting that only cyber attacks resulting in destruction could qualify as acts of cyber-terrorism (Denning, 2000). Maura Conway (2003) is more specific. Cyber-terrorism is "terrorism involving computer technology as weapon or target" rather than simply "the terrorist use of computers as facilitator of [terrorist] activities" (Conway, 2003: 38-39). This would imply that the use of ICT by 'terrorist' groups to facilitate recruitment, propaganda or other perception-management campaigns does not qualify as cyber-terrorism.

Hacktivism, a term referring to the convergence of hacking with activism and describing "operations that use hacking techniques against a target's Internet site with the intent of disrupting normal operations but not causing serious damage" (Denning, 2001:241), should also be distinguished from cyber-terrorism as in theory the severity of the damage caused is unlikely to be as significant. Examples of hacktivism include virtual sit-ins and blockades, automated email bombs, web hacks and computer breaks-in, computer viruses and worms. As hacking incidents are claimed for and/or reported in the media, hacktivist operations can generate considerable publicity for the activists and their causes (e.g. attacks by the Anonymous group) (Denning, 2001).

Some have suggested that an act of cyber-warfare should meet two additional criteria to distinguish it from cyber-terrorism. First, it should be state-sponsored. Second, it should constitute an act of war under international law, i.e. the attack is of a scale significant enough to possibly trigger a proportional military response from the targeted state (Theohary & Rollins, 2015).

So far however, distinguishing among cyber-warfare, cyber-terrorism and other cyber attacks causing significant damage can prove more difficult than anticipated given overlapping actors, motives and impact.

3.1.2 Possible effects & estimated costs

Damage to a company or organisation resulting from a cyber attack can take several forms, well beyond data breaches (see Marsh & Cabinet Office, 2015), including:

- theft of IP or other commercially sensitive information;
- business disruption or interruption;
- data and software deletion and/or destruction;
- direct financial loss (e.g. theft of funds or extortion payments);
- third party liabilities (customers, employees, shareholders' actions) and regulatory actions;
- reputational loss;
- physical damage to people or physical assets;
- investigation and response costs;
- damage to other parties, e.g. supply chain companies, employees and private customers or members of the public.

Cyber attacks are generally presumed to be grossly under-reported. First, it can take time to detect an attack with one estimate suggesting a median of around 205 days to detect an attack in 2014 (Mandiant, 2015). Second, victims of cyber attacks have an incentive to downplay the event. Companies will tend to do so in order to protect reputation and market share. Depending on the applicable regulatory framework, identified cyber attacks resulting in data breaches can nearly automatically trigger mandatory notifications, fines and legal claims, thus reducing the incentive to report marginal attacks that might be classed as some other ICT interruption. In the case of suspected state involvement or affiliation, matters are even more sensitive. Governments do not want to appear vulnerable and will avoid making formal accusations as these can have consequences in terms of diplomatic relations, possible retaliation measures and risk of escalation. For example, NATO stated in 2014 that a cyber attack against one of its members could trigger a military response from the Alliance under Article 5 and the principle of collective defence following review by the North Atlantic Council (NATO, 2014).

Estimates of the cost of cyber crime to society range between US$400 billion to US$1 trillion. MacAfee estimates that the losses to the four largest economies (US, China, Japan and Germany) reached US$200 billion in 2014 (Center for Strategic and International Studies, 2014). In the UK, the economic cost of cyber crime is estimated at about £27 billion a year, of which about £9 billion is associated with the theft of IP from UK businesses (Detica & Cabinet Office, 2011). The average cost of data breach for a UK company in 2014 was about £2.3 million (Ponemon Institute, 2015). Such figures should be treated with caution for a variety of reasons, not least the rapidly changing situation invalidates historic numbers, the aforementioned possible under-reporting, the possibility of over-estimates by interested security parties, and the difficulties in estimating future income losses due to reputational impact or IP theft. Aside from the implications to individual companies, cyber attacks impact on the UK economy as a whole in two major ways: by increasing the cost of doing business and by distorting the pattern of long-term investment (Oxford Economics & CPNI, 2014).

3.2 Looking at the evidence

Recent evidence of cyber attacks illustrates the dynamic and fast evolving nature of the threat. Frequency and sophistication are on the rise. Besides data breaches, cyber attacks targeting infrastructure and other equipment through the disruption or destruction of industrial control systems are emerging (for example, a 2014 attack on industrial control systems at a steel mill in Germany (see Zetter, 2015)). Cyber espionage at scale is also on the rise as illustrated by charges brought against Chinese hackers in the US (see FBI, 2014). In short, cyber attacks can deliver similar destructive capacity to traditional physical assaults, including the potential prospect of multiple casualties and severe loss of public confidence.

Figure 2 – Evidence of cyber attacks

	Estonia (2007 to 2008)	Myanmar (2010)	Stuxnet (Iran) (2008 to 2010)	Sony Pictures Entertainment (2014)	Steel Plant (Germany, 2014)	State-sponsored cyber-espionage (USA, 2006 to 2014)
Type of cyber attack	Distributed Denial of Service (DDoS)	DDoS	Cyber worm		Spear-phishing attack to gain access to company network and install malware	Spear-phishing attack to gain access to companies networks
Duration	< 1 month	1 to 2 months	> 2 to 3 years	1 to 3 months	-	Circa 8 years
Detection	Immediate	Immediate	One or two years later	One or two months later	-	Months or years later
Target	Government, political parties, large banks, companies	Ministry of Post and Telecommunications (main internet provider)	Iran's nuclear centrifuges (later on other infections detected)	Sony Pictures Entertainment	Unnamed steel mill in Germany	US companies (incl. nuclear power, metals and solar products industries)
Impact	Websites disabled	Internet network and traffic disruption	Physical destruction of equipment/ infrastructure through digital disruption of industrial control systems	Theft and destruction of data. Theft of unreleased products (movies). Threats of further attacks.	Physical destruction of equipment/ infrastructure through digital disruption of industrial control systems	Theft of intellectual property as well as trade secrets, client and employee data
Level of capabilities	Medium to high	-	High	Medium to high	High	Medium to high
Terminology used to describe it	Cyber warfare	-	The first cyber weapon	Cyber vandalism	Advance-persistent threat attack	Cyber espionage
Cost	-	-	-	US$41 million (investigation and remediation costs)	-	Cyber espionage of US firms cost an estimated USD 100 billion a year
Claim/ indictment/ conviction?	Yes - One perpetrator (ethnic Russian student residing in Estonia) was convicted.	-	Isreal's Mossad confirmed involvement in Stuxnet development later on.	The Guardian of Peace, a North Korean organised group claimed responsibility.	-	Yes – five Chinese hackers (officers in Unit 61398 of the Third Department of the Chinese People's Liberation Army) indicted in May 2014
State involvement	Suspected – Russia	Suspected - Burmese military government	Suspected – Israel (confirmed after the facts) and USA	Suspected – North Korea (denied involvement)	-	Suspected – China

Figure 2 on page 13 contrasts recent cases of cyber attacks based on the type of attack, the terminology used to describe it, the type of capability, the damage and cost of the attack, and the likelihood of state involvement. For a short overview of each cyber event please see *Appendix 1* (page 37).

3.3 Cyber-catastrophe: towards a definition and adequate risk mitigation

The copious literature on cyber risks contains a number of hypothetical, yet possibly catastrophic, cases such as cyber events leading to water contamination or power grid disruption at scale. A 2013 survey of the world's exchanges revealed that 89% of respondents agreed that cyber-crime in securities markets can be considered a potentially systemic risk (Tundelkar, 2013). The concentration of cyber-risk in certain sectors such as ICT is increasingly being recognised. Cambridge Centre for Risk Studies (CCRS) uses the term 'Systematically Important Technology Enterprises' (SITEs) to describe "software systems of individual technology companies underpinning a large proportion of the cyber economy", pointing to the systemic nature of their vulnerability to cyber attacks (CCRS, 2014).

It is not difficult to provide potential, highly damaging scenarios. A number of respondents were concerned that an attack on the cloud could cause business interruption at a systemic scale. Others mentioned how a cyber attack targeting GPS technology used by the marine industry could be potentially devastating giving the industry reliance on such technology. Another spoke of the systemic risk of US doctors largely using similar medical records managements systems, so figuring out how to break one system is equivalent to figuring out how to breach tens or thousands, thus the capacity to release millions of confidential patient records. One respondent stressed how cyber-risk presents the 'biggest, most systemic risk' he has come across in his 40 plus year career in insurance.

For a cyber attack to constitute a catastrophe, it would have to cause damage at scale to the point that resulting losses exceed insurers' capacity and could potentially threaten a country's security and economy. Generally, definitions of catastrophes refer to victims (deaths, injuries) and material damages (physical damages) and in some cases to loss thresholds (Papanikolou & Dequae, 2015). In insurance, at its simplest, catastrophe risk is described as "the risk that a single event, or series of events, of major magnitude, usually over a short period (often 72 hours) leads to a significant deviation in actual claims from the total expected claims" (CEA, 2007).

Cambridge Centre for Risk Studies (CCRS) defines a cyber-catastrophe as "a systemic event that can impact many organisations at the same time, causing many of them to suffer significant losses" (Ruffle *et al*., 2014). In the absence of any comprehensive framework for the risk assessment of cyber-catastrophes, CCRS built a framework to classify cyber threats on a scale of 1 to 5 according to their magnitude to underpin their stress testing of a fictional Sybil Logic Bomb (see Figure 3 on page 15). Accordingly, attacks of magnitude 4 or 5 could possibly cause a systemic impact.

Other examples of possible cyber-catastrophes include long-term data corruption and power grid disruption, both of which were recently explored in greater detail by CCRS. The Sybil Logic Bomb Stress Test Scenario (2014) explored long-term data corruption and found that it could cause global macro-economic impact (with global 5 year GDP at risk between US$4.5 and US$15 trillion depending on the variant) portending an economic downturn driven by a reduced trust in IT by business leaders, investors and consumers. Further, the damage caused by the more extreme variants of the scenarios could be as severe as the 2007 to 2012 financial crises (Ruffle *et al*., 2014).

Figure 3 – Framework for cyber threats

Magnitude Scale Value	Threat profile	Typical perpetrator profile	Motivation	Time scale	Covert-ness	Resources/ Logistics	Historic precedents
Magnitude 1 Cyber Hazard	Undirected attack using a single cyber attack technique	Lone bedroom hacker; "script kiddie"	Curiosity; notoriety	Short	Low	Low	SQL Slammer, Mafia Boy
Magnitude 2 Cyber Hazard	Directed attack on defined targets using single cyber attack technique	Group of hackers; online buddies; hacktivists	Notoriety; activism; political	Short	Medium	Low	Sony Playstation, Conficker
Magnitude 3 Cyber Hazard	Directed attack using mix of cyber attack techniques, kinetics and social engineering	Malicious insider; organised crime; "hacker-backer-casher"	Revenge; political; financial	Medium	Medium	Medium	Unlimited Operation
Magnitude 4 Cyber Hazard	As 3 but with addition of more development resources, testing facilities, increased covertness and kinetics.	Security agency in peacetime mode; Mafia grade criminal organisation	Financial; political	Long	High	High	APT1, Stuxnet
Magnitude 5 Cyber Hazard	As 4 but with military grade resources and intensity of attack.	Electronic army; nation state	Political; military	Long	High	High	

[Source: Ruffle et al., 2014: 14]

Published jointly by Lloyd's and CCRS, a second scenario – Business Blackout (2015) – explored the insurance implication of a major cyber attack, using the US power grid as an example. The report estimates the total impact to the US economy at US$243 billion, rising to more than US$1 trillion in the most extreme version of the scenario. The cyber attack scenario shows the broad range of claims (30 lines of business) that could be triggered by disruption to the US power grid, with the total amount of claims paid by the insurance industry estimated at US$21.4 billion, rising to US$71.1 billion in the most extreme version of the scenario (Lloyd's & CCRS, 2015). Comparable losses for a similar UK scenario assuming a rough 6:1 GDP ratio might be in the region of economic impact ranging from a cost of US$40 billion (£25.8 billion at £1:$1.55) to US$166 billion (£107 billion) and insurance industry costs of US$3.5 billion (£2.26 billion) to US$11.85 billion (£7.65 billion). Figure 4 below compares the magnitude of losses under the blackout scenario with insured losses relating to past catastrophic events.

Figure 4 – Estimated insured losses resulting from recent catastrophic events

Catastrophic event	Year	Insured losses
9/11	2001	US$32 billion
Hurricane Sandy	2012	US$36.9 billion
Hurricane Katrina	2005	US$80.3 billion
Business blackout scenario	?	US$21.4 billion (US$71.1 billion in extreme version)

[Source: adapted from RAND, 2004; Swiss Re, 2014; Lloyd's & CCRS, 2015]

A cyber-catastrophe does not have to be the result of a malicious act. A geomagnetic storm of similar magnitude to the solar storm of 1859 (also known as the Carrington Event) could cause catastrophic damage to society, with some estimates of social and economic costs in the range of US$1 trillion to US$2 trillion a year and suggesting that, depending on damage, full recovery could take four to ten years (National Academy of Sciences, 2008). Equally,

there are man-made electromagnetic pulse (EMP) devices and weapons that could produce a similar, malicious disabling of ICT across a city or small country.

While a cyber attack at scale – i.e. a 'black swan' or 'cyber 9/11' event - has yet to occur, it should not be an excuse for inaction. Experts increasingly assert that it is only a matter of time till such an event occurs and fear that most countries, including the UK, are ill prepared (Kaspersky quoted by Gibbs, 2014). Experts call for governments, industries and organisations to work together to better coordinate risk management. International cooperation is also needed to strengthen efforts including in relation to fight against cyber criminals (Yasuda, 2014).

Government in particular is viewed as having a crucial coordination role in introducing appropriate risk mitigation measures; encouraging active cyber-risk information sharing among industries; monitoring cyber attacks and emerging new threats; and in encouraging faster reactions from IT security companies and other relevant players against cyber attacks nationally. In the UK, government seems to be taking the cyber threat seriously (see box 2). If one considers government expenditure in cyber security as a reasonable indication, then the UK has earmarked a total of £860 million from 2011 to 2016 (UK Government, 11 December 2014), at a time when other areas of public service provision are experiencing budget cuts.

But beyond government expenditure, genuine private defence is needed to protect the UK economy. The dynamic nature of the cyber threat - tomorrow's cyber attacks are unlikely to resemble today's ones - implies that risk management and resilience should be seen as a continuous process rather than as a one-off task.

Box 2 - UK Government response to cyber threat

In the UK, government seems to be taking the cyber threat seriously. According to the National Risk Register of Civil Emergencies (2015), cyber attacks on infrastructure score 3 for overall relative impact (1 being lowest, 5 being highest score) and 'low medium' in terms of relative plausibility of occurring over the next five years. Cyber attacks on data confidentiality score 1 out of 5 for overall relative impact but are deemed to have 'high' plausibility of occurring in the next five years (Cabinet Office, 2015). A 2014 survey of information security breaches in the UK reported that in 2013 alone, 81% of large organisations and 60% of small businesses experienced a cyber security breach.

The UK Cyber Security Strategy (2011) lays out the government's four key objectives in dealing with cyber threats for the four years to 2015. These objectives can be summarised as follows:

(1) tackling cyber crime;
(2) improving cyber resilience;
(3) supporting an open, vibrant and safe cyberspace in the UK;
(4) building UK knowledge, skills and capacity to support UK cyber security objectives.

To support the government response to cyber threats, the Office of Cyber Security & Information (OCSIA) and the Cyber Security Operations Centre (CSOC) were set up in 2010 to enhance cyber security and information assurance. In addition, the UK National Computer Emergency Response Team (CERT-UK) was set up in 2014 to strengthen UK response to cyber incidents. CERT UK includes the Cyber security Information Sharing Partnership (CiSP), which allows government and industry to share information on current threats and managing incidents on a secure platform. Over 750 companies had joined CiSP as of December 2014. While information sharing on cyber-risk is encouraged, reporting cyber attacks is on a voluntary basis in the UK.

The Centre for the Protection of National Infrastructure (CPNI) coordinates the protection of national infrastructure, in close collaboration with government agencies and the nine sectors of national infrastructure identified (which include government, transport, financial services and energy). The criticality of national infrastructure in the UK is defined according to three impact dimensions: impact on delivery of national's essential services; economic impact and impact on life.

In April 2014, the government launched Cyber Essentials, a government-backed, industry-supported scheme that provides a statement of the basic technical controls all organisations should implement to mitigate cyber-risk. The scheme includes an Assurance Framework, a mechanism for organisations to demonstrate to customers, investors, insurers and other stakeholders that they have taken these essential precautions, which leads to the awarding of certificates (BIS, 2014). There are two levels of certification. Cyber Essentials requires organisations to complete a self-assessment questionnaire (13 questions) and responses can be independently reviewed by an external certifying body. Cyber Essential Plus involves the testing of systems carried out by an external certifying body, using a range of tools and techniques. From October 2014, the government requires all suppliers bidding for certain sensitive and personal information handling contracts to be certified against the Cyber Essentials scheme (UK Government, 2015). The scheme is thought to be a sensible starting point, particularly for SMEs wishing to assess their potential exposure to cyber-risk.

4. CYBER INSURANCE

Insurance is a recognised risk mitigation approach that involves the transfer of a financial risk to a third party (the insurer) that will assume the financial risk in exchange for a premium. Companies can protect themselves against damages arising from a cyber incident in three ways – self-protection, self-insurance and cyber insurance - which are not necessarily mutually exclusive. Self-protection involves the assessment and mitigation of cyber vulnerabilities in order to improve resilience. Self-insurance consists of internal investments set aside to cover potential losses. Finally, organisations can purchase cyber insurance from third parties who manage the related risks through pooling and aggregation (ENISA, 2012).

This chapter explores the third option – cyber insurance. Section 4.1 provides an overview of the cyber insurance market. Section 4.2 analyses the challenges that cyber-risk presents in terms of insurability and the related implications for the development of an insurance market. Section 4.3 lays out opportunities for further developments including how standards can support insurability and market penetration. Finally section 4.4 discusses the possible gap in coverage should a cyber-catastrophe hit the UK (or any other country for that matter).

4.1 Overview

Cyber insurance refers to insurance policies aiming to cover a range of issues relating to cyber-risks (ENISA, 2012: 8). While some products emerged in the 1990s (e.g. Errors & Omissions policies related to technology), cyber insurance is relatively 'new' in two ways. First, cyber is increasingly being viewed as a separate component, or 'class', of commercial insurance portfolios. Second, the type of cover and exposures being underwritten, as well as the wordings, continue to evolve. (Betterley, 2015)

Cyber insurance is developing as a standalone product to fill the gap where traditional insurance policies (e.g. general business liability, property damage, business interruption) do not cover cyber-risk (Biener *et al.*, 2015; see also HUB International, n.d.). Cyber insurance products can cover either or both first party and third party losses in relation to digital assets and infrastructure (see ABI, 2015; Airmic, 2012).

Generally, first party liability coverage can include:

- loss or damage to digital assets (e.g. data, software programmes);
- business interruption (BI) from network downtime;
- cyber extortion;
- customer notification expenses;
- theft of money and digital assets.

Third party insurance usually relates to data breach events and may cover:

- security, privacy breaches and related investigation (e.g. investigation, defence costs, civil damages, regulatory fines);
- multi-media liability;
- loss of third party data and related liability.

Standalone cyber insurance products increasingly tend to involve risk-mitigation both pre- and post- incident in addition to indemnity protection. Pre-breach services can include IT security evaluation services to assess potential vulnerabilities and develop mitigation plans. Post-breach services generally focus on finding and repairing areas where the cyber hack has occurred; on developing disclosure strategies to minimise reputational damage while complying with regulatory requirements; and on positioning legal services to minimise the impact of lawsuits (Standard & Poor's, 2015).

During interviews, respondents confirmed that the great majority of cyber insurance products focus on first party liability and limited third party liability in relation to data breaches. Cyber insurance increasingly includes coverage for first party business interruption but not contingent business interruption, that is business interruption suffered by third parties following a cyber attack on one organisation. Such third parties are frequently customers. Very few offered products covering property damage or bodily injury arising from a cyber attack.

Cyber insurance policies need to be tailored to the client. Company size, customer base, web presence, existing policies, and the types of data collected and stored are all determinants of policy terms and pricing (Biener *et al.*, 2015). Regardless of policy tailoring, coverage is variable and contingent on wording, definitions and exclusions. Exclusions such as cyber-terrorism or cyber-warfare relate to the motive for an attack and its perpetrator, both of which may be difficult to identify and prove as explained in Chapter 3 and confirmed by a number of respondents in the insurance sector. One of the first relevant exclusions is the Electronic Data Exclusion NMA2914 which excludes data breaches following a computer virus (NMA 2914, 2001). Most UK markets adopted the clause on subscription business in early 2001 (CEA, 2003). Respondents also mentioned how the Institute Cyber Attack Exclusion Clause (2003, reproduced below) is regularly used in standard insurance policies though it has yet to be challenged in a court of law.

> *1.1 Subject only to Clause 1.2 below, in no case shall this insurance cover loss damage liability or expense directly caused by or contributed to by or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or any electronic system.*
>
> *1.2 Where this Clause is endorsed on policies covering risks of war, civil war, revolution, rebellion, insurrection, or civil strife arising therefrom, or any hostile act by or against a belligerent power, or terrorism or any person acting from a political motive, Clause 1.1. Shall not operate to exclude losses (which would otherwise be covered) arising from the use of any computer, computer system computer software programme, or any electronic system in the launch and/or guidance system and/or firing mechanism of any weapon or missile.*

CL 380 is widely used across a broad range of marine, energy and industrial property insurance policies. A cyber attack in these sectors could be very disruptive and result in significant losses, yet the clause means that the insured are without cover for losses or damage arising from a cyber event (except for missile attack) (Mole, 2014). An example raised by some respondents was whether the clause excluded property damage where a cyber attack released the spillway controls for a dam causing extensive flooding.

As cyber-risk is not well understood, underwriters are cautious, applying relatively high deductibles, low limits and high premiums in the face of high uncertainty (see for example Biener *et al*., 2015). Average limits are difficult to confirm with certainty. Respondents reported limits to average US$50 million for larger organisations with some wishing to purchase up to US$150 to US$200 million. A recent market report on cyber insurance by Marsh (2015) shows that average cyber liability for companies with revenue exceeding US$1 billion in the US was US$34.1 million in 2014 (compared to US$27.8 million in 2013), suggesting that while limits may be rising, only a few approach or exceed US$50 million (Marsh, 2015). Standard & Poor's (2015) mentions limits in the US averaging US$25,000 for SMEs, up to US$5 to US$25 million for larger companies.

Cyber insurance premiums relative to the limit purchased were found to be three times higher than for general liability and six times higher than for property (Marsh & Cabinet

Office, 2015). While the insurance industry seems to be looking for better segmentation models to price cyber exposure appropriately, there appears to be little differentiation in pricing from one insured to the other reflecting the lack of data (Marsh, 2015). As an industry market report reveals "insurers [currently] seem to be underwriting and managing loss potential not by individual account selection and pricing disparity, but by controlling aggregate loss potential through limits constraints according to industry, geography, and total amount of cyber coverage offered" (Marsh, 2015:2). In short, insurance appears to be comparatively expensive and not priced according to the client's actual risk.

The size of the market is difficult to assess. In the USA, the Betterley report (2014) states gross written premiums (GWP) totalling as much as US$2 billion in 2014 (compared to US$1.3 billion in 2013). Lloyd's estimates the growth of the American market to US$2.5 billion GWP in 2014 from less than US$1 billion in 2012 (Standard & Poor's, 2015). The European market in contrast was deemed to be worth between US$150 and US$200 million in 2013, with an estimated 50% to 100% annual growth rate and expectations that GWP could possibly amount to US$1.1 billion by 2018 (LMG, 2014; see also Biener *et al.*, 2015).

Market penetration is relatively low and uneven. Respondents highlighted that the majority of the exposure is currently concentrated in the US (as much as 95%), driven by data breach notification laws and the high cost of dealing with security breaches (of which legal fees is a big component). Asia is likely to follow with a 25% growth in 2014. In Europe, it is expected that demand will grow following updates to the European directive on data protection and the introduction of a new directive on information network security (Reactions, 2014; ENISA, 2012). In terms of sectors, the majority of cyber insurance seems to be purchased for data breaches by organisations operating in retail, healthcare, hospitality and financial services (ENISA, 2012). However, data breach insurance covers a narrow area of administrative cost risk, not property damage, business interruption, or third party liability.

To contrast penetration in the US and in the UK, a British market research firm report cited on the MunichRe website stated that 30% of major US companies have already bought cover against cyber-risk, compared with only 5% of companies in Europe (MunichRe, n.d.) In the US, penetration of cyber insurance is estimated at 16% across all sectors with higher penetration in health care (50%), education (32%) and hospitality (26%) (Statista, 2015). In the UK, while a survey revealed that 52% of CEOs and CIOs of large organisations believed they have insurance that would cover them in the event of a cyber breach, the recent report from Marsh & Cabinet Office suggests that actual penetration for standalone cyber insurance might be as low as 2% for large organisations and close to nil for SMEs (Marsh & Cabinet Office, 2015; BIS, 2014). A 2014 UK and Ireland survey indicated by contrast that 51% of companies had either bought cyber insurance or were planning to seek quotes against 49% who did not. Surveyed organisations were primarily concerned by losses arising from the breach of customer information (52%), followed by business interruption (30%), and IP theft (9%). (Marsh, 2014)

4.2 Challenges: questioning cyber-risk insurability

"*So far the insurance industry considers cybercrime as borderline insurable, quite similar to terrorism*"
(Liès, 2015:1)

Cyber-risk issues that challenge insurability and market development include the lack of actuarial data; difficulties in pricing; uncertainty around what is covered (wording and exclusions) and what the clients think they are buying; aggregation risk catastrophe models and the potential lack of adequate reinsurance capacity.

While many insurance markets have begun with little or no data, insurers like data, and more and better data leads to better pricing and a better market. Respondents all agreed that the lack of data, both on attacks and related losses, could exacerbate adverse selection and moral hazard. Organisations[1] such as Ponemon Institute, FireEye and Verizon already provide useful information and data on cyber attacks, their type and impact. One respondent suggested that ICT firms who review data from millions of computers and servers could also provide reliable data on cyber attacks, including on the means used for the attacks and their success rate. Some respondents wanted government and insurers to collaborate more on secure information sharing to support modelling, while others questioned whether government had much data worth sharing. While, with more data, current natural catastrophe analysis, such as that provided by PERILS, could be replicated for cyber events, some respondents claimed that historical data (attacks and losses) will only ever be partially relevant given the dynamic nature of cyber-risk, with new technologies and devices being used to carry out attacks and thus altering impacts and losses (Biener *et al*., 2015; ENISA, 2012; Standard & Poor's, 2015).

Cyber insurance products are often described as costly and not necessarily priced on risk, as highlighted in the previous section. The process of pricing cyber-risk can be informed by several variables including the number of sensitive records; what the records contain; the use of encryption, firewall, and other defences; the extent of potential regulatory cost exposure; IT security controls in place and prior losses. However, as one respondent said "pricing cyber insurance remains very much a judgement call". This is partly due to the novelty of the product, which has implications for risk pooling, insurance product supply and data availability. Equally, cyber-risk entails significant information asymmetries that require costly verification and upfront risk assessment. (Biener *et al*., 2015)

Coverage uncertainty exists both with 'standard' policies and standalone cyber policies. This is partly the result of coverage heterogeneity, inconsistent wording, varying definitions of the risk(s) and the use of exclusions (e.g. London Market Cyber Attack Exclusion (CL380) and the Electronic Data Exclusion (NMA2914)). Coverage uncertainty is aggravated by the interaction and overlap with standard insurance products and the extent to which property, liability and specialty cover for example would respond to cyber events (Yasuda, 2014). Uncertainty also exists under standard exclusions on war and terrorism given how attribution of malicious cyber events can prove difficult and the unlikelihood of such events being classified as acts of war or terrorism by states (CRO Forum, 2014). On the other hand, one could argue that coverage uncertainty also relates to difficulties in assessing possible secondary (indirect) losses most notably in relation to 'soft assets' (e.g. reputation) (LMG & BCG, 2014; Biener *et al*., 2015). Such losses are likely to depend on a number of factors including the industry, the size of the organisation and whether organisations are publicly listed or not (ENISA, 2012).

Several respondents highlighted the need for standard policy wording in relation to cyber attacks and suggested that it should be an industry-wide initiative. Such undertaking should not only consider a common definition of cyber events, risks and damages covered, but also include the interests of the cover that are specifically excluded under a cyber policy.

The lack of product consistency can in turn lead to trust issues, i.e. trust in the insurer that he will pay the claim in the event of a cyber breach or attack. Some question whether the limited capacity being offered and limited take up of existing products is because products fail to match customer needs and to add value (Russell, 2014; Tendulkar, 2013). A survey of chief information security officers revealed that of those who had cyber insurance (26%), 48% were not convinced that insurers would pay in the event of claim (KPMG, 2015).

[1] See for example FireEye's Threat Intelligence Reports ; Ponemon's research studies and white papers and Verizon's 2015 Data Breach Investigation Report

Another survey reported that 31% of participating organisations indicated that the insurance available did not or did only partially meet their needs, against 12% who said it fully met their needs (Marsh, 2014). Finally, the lack of availability, prohibitive cost, coverage with limitations were often cited by exchanges who did not have insurance (78%, against 22% who did have cyber insurance) (Tendulkar, 2013).

Aggregation was cited as probably the most pressing issue impeding insurers from assessing adequately the maximum possible loss they could incur and the amount of cover they can provide. Aggregation and clashes can occur when:

- one cyber event triggers multiple claims by one customer under different policies (for example Property Damage and Directors Errors & Omissions); or,
- one cyber event triggers multiple claims by multiple clients under different policies (catastrophe loss); or,
- the initial claim investigation determines multiple past attacks over a number of underwriting years of account triggering multiple claims across potentially multiple different underwriters.

Aggregation is exacerbated by the interdependence of cyber-risks. As many organisations use similar software, security programmes and other ICT infrastructure (what some termed 'monoculture'), a successful attack on one (e.g. Distributed Denial of Service (DDoS)) implies that others are vulnerable to the same attack. The rapid adoption of cloud services further aggravates the problem of interconnectivity. Diversification of cyber-risk exposure by industry, counterparty and geography may as a result not be as straightforward. Independent risk pools can be difficult to achieve, thus questioning the insurability of cyber-risk in the first place. (ENISA, 2012; Biener *et al*., 2015; CRO Forum 2014)

While aggregation issues are not new, aggregation can be more difficult to assess in the case of cyber-risk given the lack of historical loss data and the dynamic nature of the risk (Yasuda, 2014). Uncertainty around the maximum possible loss and the risk of aggregation can lead to possibly inaccurate estimates of the actual risk on insurers' books. To some extent, exclusions attempt to manage the risk of aggregated losses.

Some respondents highlighted two trends in the insurance market which could potentially lead to further unknown cyber aggregation. First, some reported how underwriters are being encouraged by brokers to include cyber coverage as part of Property Damage policies. Second, due to the nature of a soft insurance market, underwriters are in some cases removing exclusions such as CL380 and/or providing 'small cyber limits' in order to retain business. Both cases could lead to additional challenges in trying to estimate the overall exposure to cyber-risk across policies.

Total exposure of the insurance industry remains in fact difficult to estimate. The Marsh & Cabinet Office report (2015: 23) estimated that: "in 2014, the global exposure of the insurance industry to cyber-risk (as quantified by the total of standalone cyber indemnity limit sold) stood at around £100 billion. Assuming that the possible maximum loss (PML) follows the range for property risk (up to 20% of the total exposure), the insurance industry could face a cyber PML of up to £20 billion. If we consider that the cyber insurance market could treble in the next three to five years, the industry PML for cyber-risks could easily exceed the global insurance/reinsurance capacity available for other aggregating events, such as nuclear disaster (£3 billion) or natural catastrophe (£65 billion)."

The lack of reinsurance is perceived as a major obstacle to cyber insurance market development. Without appropriate reinsurance, insurers cannot provide regulators with assurance that they do not risk failure. Respondents suggested that more work is needed to understand and assess the risk of accumulated losses across policies and clients and that this should better take place before a cyber catastrophic event hits somewhere. As Chapter

5 explores in greater detail, existing reinsurance options for cyber insurance are limited. Lack of reinsurance can prevent market development by inhibiting both supply (i.e. low capacity available) and demand (e.g. perception of insurers' ability to pay a large claim) for cyber insurance (ENISA, 2012).

Other often-cited challenges in cyber insurance include the lack of cyber expertise among brokers and underwriters preventing them from selling dedicated products or writing cyber-risk as well as the lack of a shared understanding of cyber-risk(s) and event definitions. Some insurance respondents noted a lack of demand from insurance clients, either because clients do not take cyber-risk seriously or due to insurance products not fully addressing clients' needs (e.g. in terms of coverage and limits). Other insurance respondents thought there was a chicken-and-egg problem. Clients found existing levels of insurance and terms expensive or derisory and had stopped seeking cover.

4.3 Opportunities for cyber-risk mitigation

Insurance is increasingly seen as part of the toolkit to manage cyber-risk exposure. The Marsh & Cabinet Office report (2015) pointed out that the insurance industry can help to mitigate the risk in several ways:

- by putting a cost on a firm's cyber-risk through the premiums they pay and encouraging policy holders to take steps to mitigate the risk;
- by reducing losses through information sharing on cyber-risk and related data;
- by sharing risk management expertise as many aspects of cyber-risk, such as business interruption, potential for large and public impact, are common to other tail risks such as natural catastrophes and terrorism.

Some respondents looked to insurance to bring appropriate market forces to bear on improving cyber standards, products and services. Based on the above, three areas could support cyber insurance development and take up. These include:

- improved disclosure of cyber-risks and events;
- standards for cyber security and resilience;
- testing the vulnerability of large organisations in sectors of national importance.

4.3.1 Disclosure of cyber-risks and events

Improved disclosure of cyber-risks and events can not only help information sharing but can also drive risk assessment within organisations, large or small, across sectors. In the UK, the Cyber security Information Sharing Partnership (CiSP) allows government and industry to share information on current threats and to manage incidents on a secure platform. Over 750 companies had joined CiSP as of December 2014. While information sharing on cyber-risk is encouraged, reporting cyber attacks is on a voluntary basis in the UK. In the US, besides data breach notifications laws, SEC guidance on disclosure for cyber security encourages publicly traded companies to disclose significant instances of cyber-risks and events (Hartwig & Wilkinson, 2014).

Regulation could mandate disclosure, particularly for large organisations (not only publicly traded ones) operating in critical sectors of activity such as financial services, transport and energy. Disclosure should include the reporting of both unsuccessful and successful attacks, and estimates of possible financial losses following an attack, as well as appropriate risk mitigation measures being taken, including insurance.

4.3.2 Voluntary standards on cyber security

Cyber standards do exist. From the early 1990s standards such as the UK's ITSEC led to DISC PD003, to BS 7799, to ISO 17799, and finally to the ISO 27000 standards. ISO/IEC 27001 (2013) is widely recognised as an international standard which specifies a management system to bring information security under explicit management control. Within

the same family of standards ISO/IEC 27032 (2012) provides guidance for improving the state of cyber security, drawing out the unique aspects of that activity and its dependencies on other security domains such as information security, network security, internet security and critical information infrastructure protection.

In the UK, Cyber Essentials, a government-backed, industry-supported scheme that provides a statement of the basic technical controls all organisations should implement to mitigate the cyber-risk, was launched in 2014. The scheme includes certification and is thought to be a good starting point in assessing cyber vulnerabilities, particularly for SMEs but less so for large and more complex organisations.

In the USA, following the President's Executive Order 13636 (Obama, 2013), the National Institute of Standards and Technology (NIST) developed a voluntary Framework for Improving Critical Infrastructure Cybersecurity in collaboration with government and industry. The Framework Core (Part I) is a set of cyber security activities, outcomes, and informative references that are common across critical infrastructure sectors. The Core includes guidance for individual organisations to develop their Profile (part II), to help them align cyber security activities with business requirements, risk tolerances and resources. Finally, the Tiers provide a mechanism for organisations to view and understand the characteristics of their approach to managing cyber security risk (NIST, 2014).

Voluntary standards on cyber security can directly support risk assessment and the implementation of mitigation measures which in turn contribute to improving cyber resilience. Standards are regularly reviewed over time to ensure that they remain fit for purpose. This is particularly relevant in the case of cyber security as the cyber threat can evolve fairly rapidly over time. The majority of respondents agreed that standards could provide a common framework to assess and manage risk and could improve business understanding of cyber-risk. Successful certification under designated standards could in turn inform the underwriting process for cyber insurance and perhaps translate into discounted premiums for smaller organisations in sectors other than ICT. Some respondents suggested that the adoption of standards could be mandated for organisations operating in sectors of national importance and related suppliers (e.g. cloud service suppliers) to ensure common frameworks of risk assessment and mitigation. A few respondents worried that standard-driven risk assessments are at best subjective and could fail to reflect accurately organisational performance in cyber resilience. While standards and related certification have a role in informing the underwriting of cyber-risk, this would suggest that pre-bind cyber-risk assessments are likely to remain important for standalone cyber insurance for large organisations in particular.

Standards now need to evolve alongside proof of their value-added. Over time, insurers are likely to promote those standards that prove most effective in assessing and reducing risk by encouraging positive behavioural changes in organisations.

4.3.3 Vulnerability testing large organisations in sectors of national importance

Vulnerability testing against cyber threats of catastrophic nature is also developing. In the UK, CBEST Vulnerability Testing Framework, an initiative of the Bank of England in collaboration with the Council for Registered Ethical Security Testers (CREST), provides a framework to deliver cyber security tests for systematically important financial institutions (SIFIs). As Andrew Gracie said at the public launch of the scheme on 10 June 2014: "the idea of CBEST is to bring together the best available threat intelligence from government and elsewhere, tailored to the business model and operations of individual firms, to be delivered in live red team tests, within a controlled testing environment." (Gracie, 2014: 3) CBEST is a voluntary scheme though participation by SIFIs is strongly encouraged.

On 1 July 2015, the Prudential Regulatory Authority (PRA) sent a request to the UK's largest general insurers to participate in a stress test exercise covering a wide range of events including cyber loss – General Insurance Stress Test 2015. The scenario specification for cyber loss entails "a series of simultaneous cyber attacks launched on large multinational organisations and discovered across the Retail sector with the intention of causing major disruption and financial loss to organisations" (PRA, 2015: 30). The scenario assumes that the 15 largest clients of an insurer are targeted and requires estimated losses to be considered across cyber policies and under other policies such as Errors &Omissions policies with cyber endorsements; crime; general liability; and other policies that may respond (PRA, 2015). This test addresses exclusions, "Where an Electronic Data Exclusion or a Cyber Attack Exclusion clause has been consistently applied to a non-cyber specific (Other) policy, a zero gross loss incurred may be assumed for that line of business. If however such clauses have NOT been consistently applied across that line of business, a minimum 90% limit loss must be assumed" (PRA, 2015:29). And addresses reinsurance, "For reinsurance purposes please calculate separately on the basis that these attacks are deemed both as one event and as fifteen separate events, returning whichever causes the largest net loss." (PRA, 2015: 29) By late this year, this stress test will inform calculations of the insurance and reinsurance exposure to cyber-risk.

Similar stress testing exercises could be extended to large organisations operating in sectors of national importance. One way to develop this would be to invite infrastructure assets and operating organisations viewed as 'critical' by CPNI to participate in each of the nine sectors identified namely communications; emergency services; energy; financial services; food; government; health; transport and water. As cyber attacks on infrastructure are being reported, such an exercise would inform risk management protocols and internal calculations of possible losses following a cyber attack.

Assessment tools are also being developed to assist organisations in better decision-making regarding their Cyber defences. These are not necessarily focused on compliance but consider the overall effectiveness of the defences in place. One such tool is CDCAT[2], which provides a snapshot of the maturity of an organisation's technical and non-technical controls thereby helping an insurer form a clearer understanding of the financial risks.

4.4 Future outlook: mind the gap

Overall, cyber insurance is seen as a profitable undertaking offering great prospects for the future. Some, like Swiss Re, anticipate that by 2025 cyber coverage will be in every retail, commercial and industrial insurance policy (Liès, 2015). According to Guy Carpenter (2015) the global cyber insurance market is worth about US$2 billion and is expected to grow to approximately US$5 billion over the next five years.

Nevertheless, the gap in coverage and sectors insured should not be underestimated. Most cyber products focus on digital assets and data breaches as well as breach response and crisis management. Business interruption is rarely included. Property damage and bodily injury are generally excluded. Only a few cyber insurance products were found to cover either property damage and/or business interruption.

Many insurers pondered whether cyber was a "separate class of insurance", i.e. was it or should it be covered under existing policies, or should the industry create separate policies. This was a topic of considerable discussion. Much of the discussion hinged on whether the cyber exclusion clauses were (a) being applied in the market and (b) enforceable. The

[2] CDCAT was developed by DstL and it has been developed for commercial use by APMG under contract to Ploughshare innovations/DstL.

General Insurance Stress Test 2015 mentioned in the previous section will determine whether the exclusion is being used. If the exclusions are widely and successfully used, then cyber is more likely to emerge as a separate class. As a separate class, cyber-catastrophe reinsurance will help the market grow more safely and rapidly. If exclusions are not being widely used or are possibly overturned, then general insurers may need cyber-catastrophe reinsurance already.

Stiff regulatory capital requirements impede, correctly, insurers taking on too much exposure in the event such aggregation overwhelms them. At the same time, these requirements impede the ability of insurers to write 'normal' property damage, business interruption, and third party liability cover without excluding cyber events.

As one respondent pointed out, "customers are not always looking for what they should be looking for". The use of cyber exclusions in sectors such as the marine and energy industries raises significant concerns about critical asset protection and business interruption as well as the potential for highly correlated losses that could arise following a major cyber attack. Large organisations in these sectors require higher limits than currently available. Some respondents pointed out how some organisations are favouring self-insurance (including captive insurance[3]) over cyber insurance, as existing products do not necessarily match their requirements. The possible threat of a cyber-catastrophe undermining the UK economy and security suggest encouraging strongly (or mandating) vulnerability assessments and insurance for critical infrastructure assets and related organisations in defined sectors.

The lack of cover and the use of exclusions leave most businesses completely uninsured against bodily injury, property damage and business interruption resulting from a cyber attack. Should a cyber-catastrophe occur, this could have dire consequences for the UK economy and probably involve some government intervention to maintain critical functions and services. Insurance industry players recently warned that a cyber attack that hits several industries could lead to individual insurer insolvencies without a government backstop (Reactions, 2015). At the same time, removing exclusions would leave insurers exposed to substantial 'net' losses too, a tendency aggravated by the lack of adequate reinsurance.

Respondents noted that the London Insurance Market does not fully understand the potential consequential loss following a large cyber attack for example targeting the national power grid. Modelling exercises such as those carried out by CCRS (see CCRS, 2014 and Lloyd's & CCRS, 2015) in conjunction with the insurance industry and the upcoming stress testing exercise involving large UK insurers should inform the process of assessing the insurance industry exposure to cyber catastrophic risk. More work is needed however to define what level of losses constitutes a cyber catastrophic event for a country like the UK regardless of cause, effect or intent.

Finally, the interconnected nature of ICT infrastructure and the internationalisation of supply chains illustrate the possible global nature of cyber-risk. Thus, a coordinated approach towards mitigating cyber catastrophic risk should not only rely on public-private cooperation within the UK but should consider international cooperation as well.

[3] A recent AON study (2014) revealed however that only 1% of captive owners are funding cyber-risk through their captives, with the majority of captives writing cyber-risk being from US healthcare industry following Obamacare (Aon, 2014)

5. TOWARDS PUBLIC-PRIVATE CYBER-CATASTROPHE REINSURANCE

Reinsurance provides a risk transfer mechanism within the insurance industry allowing for a portion of primary insurers' risks to be transferred to specialist companies. Reinsurance is one of three ways through which insurers can 'externalise' part of the risk on their balance sheet, alongside securitization (e.g. insurance-linked securities), and the use of derivatives (CSFI, 2014). Reinsurance is a pooling system for insurers.

This chapter is divided in three parts. Section 5.1 provides an overview of existing cyber reinsurance options and explores the relevance of alternatives to reinsurance such as insurance-linked securities (ILS). Section 5.2 elaborates a possible approach for a public-private cyber-catastrophe reinsurance scheme either as a standalone or by extending an existing public-private scheme. Finally, section 5.3 analyses respondents' views on both the role of government and the relevance of a public-private cyber-catastrophe reinsurance scheme.

5.1 Existing reinsurance options

According to industry reports (see, for example, Standard & Poor's, 2015), most cyber reinsurance is embedded in complementary treaties like Specialty Casualty, Errors & Omissions or Directors & Officers treaties on a quota-share basis rather than under cyber standalone reinsurance treaties. Quota-share reinsurance is often used with new risks and consists of "a type of pro-rata insurance in which the primary insurer and the reinsurer share the amounts of insurance, policy premiums, and losses" (CPCU, 2013: 2.5).

Many respondents emphasized the limited availability, fairly expensive price and restricted coverage of standalone cyber reinsurance treaties. They noted the narrowly defined wording that defines an event under a cyber standalone reinsurance policy. One example mentioned was that the mutation of a known cyber virus would not be covered by a well-known policy whereas a brand new virus could be covered by the same reinsurance policy.

Concerns over cyber modelling and aggregation risks are prompting reinsurers to place sub-limited coverage, attachment-point restrictions, event limits and exclusions (such as social networking, online gaming, public entities and universities) when they offer cyber reinsurance coverage as part of broader treaties (Standard & Poor's, 2015). Respondents confirmed this trend and noted the use of cyber exclusions in broader reinsurance treaties.

Many respondents worry about the difficulty of accessing adequate cyber reinsurance coverage citing the relatively higher price and limited cover. Yet, several respondents stated that they were able to access adequate reinsurance cover for their cyber book. One in particular said they had not encountered any issues in obtaining reinsurance given that the spread of risk between their large and diverse cyber book and other classes of businesses they cover satisfied their reinsurers. This would suggest that obtaining reinsurance might be more complicated for insurers that either have a small book of cyber business or come in and out of the class.

Many respondents were concerned about their cyber-risk exposure under other lines of business or via their reinsurance activities. Several respondents from the insurance industry were concerned with exposure to sideways incidents through the accumulation of net lines. Difference-in-Conditions (DIC) insurance is one way to bridge the gap between standard policies and a number of different perils. One respondent did mention that he had bought DIC insurance to protect his syndicate reinsurance programme against cyber-risk.

The issuance of insurance-linked securities (ILS) is increasingly discussed as a relevant option to complement cyber reinsurance capacity. A risk transfer mechanism from the originators of insurance to investors, an ILS involves the creation of a special purpose vehicle which undertakes the securitization of a specific block of reinsurance by issuing securities, usually with a maximum maturity of three years, to investors. Securitization enables the diversification of risk and the amelioration of concentrations. The proceeds of the issuance are invested and the collateral is available to meet the relevant reinsurance claims (CSFI, 2014). Extreme index movements can trigger some ILS's. To date, ILS's have been mostly issued in the form of 'catastrophe bonds' in several schemes, such as extreme wind or flood or longevity.

If cyber-catastrophe 'events' could be defined, e.g. "more than 10% of the nation's computers unusable for more than 12 hours", "a power loss of more than one hour for more than 15% of the nation", or "the XYZ Cyber-Attack Index goes above 900 points for a full day", and such events could be strongly linked to cyber cover being written, then ILS's are theoretically suitable. Cyber-catastrophe bonds (i.e. cyber-catastrophe ILS) would thus represent 'event-driven' risks with binary outcomes over a defined time period. Cyber ILS pricing is likely however to be relatively higher as it will have to have to reflect a significant margin of uncertainty given the lack of historical data (CRO Forum, 2014). While a few respondents ventured that cyber-catastrophe bonds might be attractive, there were significant doubts about how readily these might be issued and at what rates. ILS's were seen as an attractive medium- to longer-term feature.

Overall, as the cyber insurance market matures, reinsurance capacity is likely to rise. At the same time, however, the lack of adequate reinsurance limits market development for cyber insurance given limited capacity and restrictive coverage. While the insurance and reinsurance industry should work together to assess cyber-risk exposure across policies and to shape a standard definition of cyber coverage, there are limits to the role the industry can play in managing systemic risk until it is much larger. In fact, the absence of an insurer of last resort to reinsure catastrophic risks is seen as part of the problem of failing to provide sufficient cyber insurance protection through insurance and reinsurance (CRO Forum, 2014; ENISA, 2012).

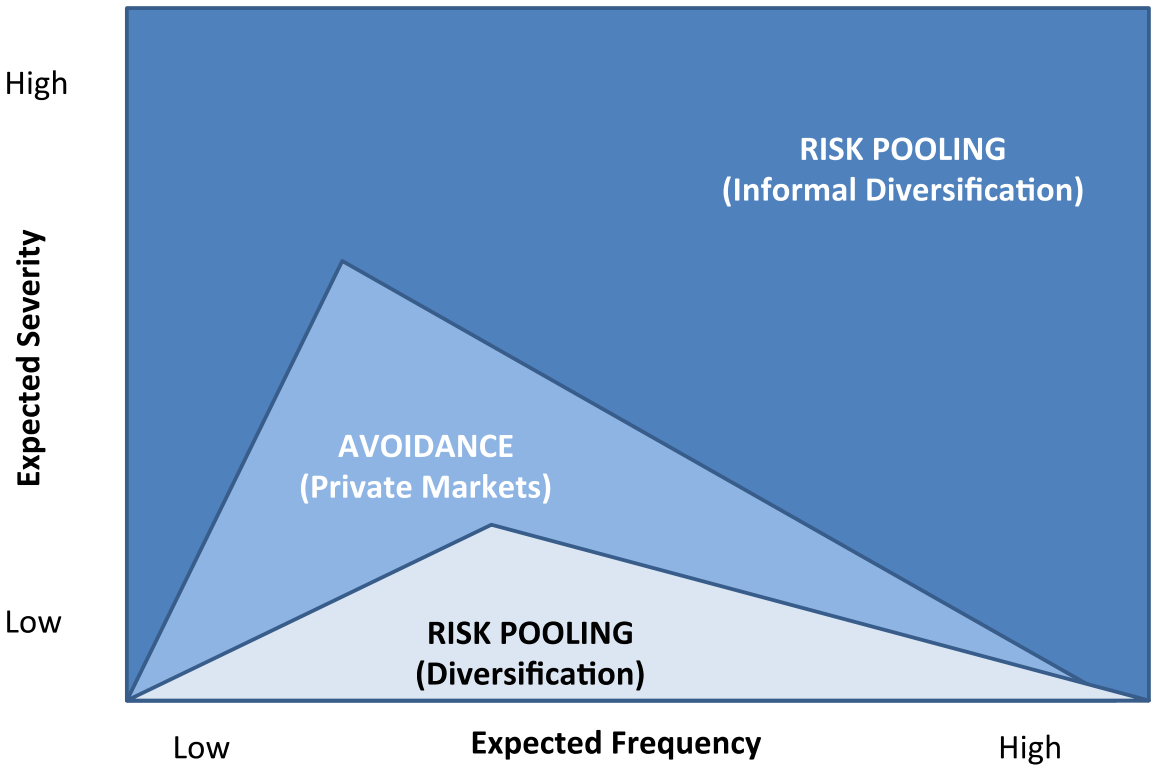
5.2 Towards a public-private cyber-catastrophe scheme: a possible approach

Three trends are (or should be) a source of concern. First, the insurance industry balance sheet does not seem to have the capacity to deal with a cyber catastrophic event. Second, existing cyber insurance is likely to cover only a portion of losses associated with a cyber-catastrophe given the focus of cyber products on data breaches and network disruption and the use of exclusions. This would therefore leave a major portion of the losses resulting from a cyber-catastrophe uninsured. Third, the UK government is unlikely to back a reinsurer yet face unlimited liability in the event of a cyber-catastrophe affecting the country at scale. Taken together, all three issues should lead to the conclusion that government and the insurance industry should be working out a framework now. Such a framework should provide the right coverage to the right people thus giving resilience and protection to the UK economy and supporting cyber prosperity. As one respondent pointed out, the last thing one would want is for the insurance industry to assume that government would deal with losses resulting from a cyber-catastrophe event.

As Michael Powers (2012: 168-169) suggests: "Unlike an insurance company, a national government cannot actually avoid any particular category of risk. Therefore, all exposures in the top-most region (with high expected severities, whether associated with low or high expected frequencies) must be accepted, albeit reluctantly by government. However, because of the political difficulty associated with setting aside sufficient financial reserves for

these costliest of exposures, the government will tend to address them only as they occur, on a pay-as-you-go basis. In the bottom-most region, the government can take advantage of the likely presence of many similar and uncorrelated claims with low expected severities, so this region is much like the corresponding region for insurance companies. Here, the government sets aside formal reserves for various social insurance programmes (e.g. pensions, health insurance and unemployment/disability benefits). Finally, in the middle region, the government typically tries its best to avoid these risks by encouraging firms and individuals to rely on their own private insurance products (but naturally, does not always succeed)."

Figure 5 – Government approach to risk finance



[Source: Adapted from Powers, 2012: 168-169]

Based on Figure 5, the major issue for the UK appears to be the limited willingness to cover certain insurable elements of cyber-risks by the insurance industry (in the bottom and middle region) given high uncertainty not only regarding risk exposure and upper bound loss but also with respect to who would bear the losses resulting from a cyber-catastrophe event (corresponding to the top region).

Existing best practice of catastrophic risk management in relation to terrorism suggests that a reasonable course of action could be to design a public-private partnership where the government acts as 'an insurer of last resort' once the insurers' retentions and the pool funds are exhausted.

Two existing UK schemes were cited as similar examples of public-private reinsurance, Pool Re (see Box 3 on page 33) and Flood Re (see Box 4 on page 34). Pool Re provides reinsurance cover for losses resulting from damage to commercial property and business interruption following a terrorist attack. Pool Re has paid a number of claims since 1993 though government financial support has not been required. Flood Re has been recently established as a separate scheme to enable flood cover to be affordable for those households at highest risk of flooding and ensure home insurance availability. While both

are interesting models to consider, Pool Re is a catastrophe scheme, which has successfully demonstrated how such a public-private cyber-catastrophe reinsurance scheme could work. Flood Re is a scheme about making existing cover more affordable for a known peril. It is probably not as relevant in structure, though it does indicate how government and the insurance industry can work together. Respondents speculated that a final structure might be quite similar to Pool Re, or an extension of Pool Re.

At its simplest, a public-private cyber-catastrophe reinsurance scheme would provide reinsurance cover for losses resulting from a cyber-catastrophe and exceeding a certain level. Some respondents suggested that this excess point could be in a region above £200 million per participant, though government and the insurance industry should agree on a precise threshold. In the UK, the scheme could either run independently as a 'Cyber Re' or, as the majority of respondents suggested, by extending the remit of Pool Re to manage cyber-catastrophe cover under a separate scheme. Extending Pool Re could prove more effective as the scheme already has a successful track record of reinsuring against terrorism; already has relevant membership from the insurance industry; has experience of managing financial reserves and is credible in the market should it decide for example to issue ILS.

Such a scheme would be a world first. Some existing terrorism risk insurance programmes in the world cover cyber-risk either by default because no exclusions have been made (e.g. France's CCR), or partly under existing criteria for cover (e.g. USA's TRIA). For more information, *Appendix 2* (page 40) compares terrorism risk insurance programmes in selected countries based on their scope of coverage, the role of government and the extent to which cyber-risk is included or not in the cover. A UK public-private cyber-catastrophe reinsurance scheme would though be one with the most clarity since it would be both specific and rely on pre-funding. Such pre-financing would in turn relieve the burden on government (and thus on tax payers) should a cyber catastrophe arise and transfer the risk to the (re)insurance market which has expertise of dealing with catastrophic risk and associated claims.

Benefits of a cyber-catastrophe reinsurance scheme are likely to outweigh the costs of development. Anticipated benefits are likely to include more clarity and certainty around the role of the government and the contribution of insurers to the pool. Several respondents mentioned that the availability of such a public-private reinsurance solution would support market development by removing cyber-risk exclusions from insurance policies and driving standard cyber coverage and wording. Moreover, the scheme would not only improve UK cyber resilience but also UK competitiveness as an attractive economy to locate cyber business where cyber-risks are being managed, and a place to source cyber-risk and security experts who have proven their financial, as well as technical, prowess, something which is a stated aim of the government.

Any attempt to develop a public-private cyber-catastrophe reinsurance scheme in the UK should be decided jointly between government and the insurance industry, possibly including consultation with other relevant industries.

Box 3 – Pool Re

Pool Re was set up in 1993 by the insurance industry in cooperation with the UK Government in the wake of the IRA bombing campaign on the UK Mainland. The cost of the losses associated with terrorism incidents in the early 1990s caused insurers and reinsurers to focus on the difficulties of providing terrorism cover for commercial properties, in particular the high potential cost of losses and the lack of any reliable method of estimating what the future loss experience might be. A withdrawal of terrorism insurance could potentially have had serious consequences for the UK economy. A new mechanism, involving both the industry and government, was therefore needed for providing this type of cover without leaving insurers or reinsurers open to substantial losses for which there was no reliable method of calculation accurate premiums.

Pool Re is a mutual reinsurer operating as a public-private partnership to reinsure property damage and business interruption against terrorism in Great Britain. Membership is open to any insurer authorised to insure losses arising from damage to commercial property located in England, Scotland and Wales. Pool Re Members comprise the vast majority of insurers and Lloyd's Syndicates which offer commercial property insurance in the UK. The Scheme provides a guarantee, which ensures that Members can provide cover for losses resulting from acts of terrorism, regardless of the scale of the claims. The Scheme is owned by its Members but is underpinned by a HM Treasury commitment to support Pool Re if ever it has insufficient funds to pay a legitimate claim. Under Pool Re's Retrocession Agreement with HM Treasury, Pool Re is required to pay a premium for this protection to the Treasury. Any amounts claimed by Pool Re under the Retrocession Agreement have to be subsequently repaid to the Treasury.

The Scheme has adapted to changing circumstances in the insurance market, in particular following the attacks in America on 11 September 2001. Pool Re's cover to insurers was originally restricted to damage caused by acts involving fire or explosion with the international reinsurance market covering other types of terrorism. In 2002, an agreement was reached to extend the cover to an 'all risks' basis, no longer restricted to fire or explosion. Exclusions relating to chemical, biological, radiological or nuclear attacks were also removed. The only admissible exclusions to the terrorism cover provided by Members are in respect of war and related risks; and damage to computer systems caused by virus, hacking and similar actions.

Under the arrangements, the government (HM Treasury) undertakes to issue a certificate whenever a particular event is deemed to be an Act of Terrorism although there is a facility to refer to an independent tribunal in cases of dispute over the certification of a particular event as an Act of Terrorism. The tribunal's decision is binding on all parties. Pool Re responds to claims only where such a certificate has been issued.

Under the Pool Re scheme, the reinsurance cover provided to Members is subject to a maximum loss retention per event per member (or members forming part of a Group) combined with an annual aggregate limit. The amounts of the retentions are based on the extent of Members' participation in the Pool Re scheme. The retention for each insurer is set annually, as a proportion of an industry-wide figure and advised to Members before the start of the relevant underwriting year. The industry wide figures have remained unaltered since 2006. They are currently £100 million for calculating the per event retention and £200 million for calculating the annual aggregate retention, subject to minimum retentions per member of £100,000 and £200,000 respectively net of any premiums paid by Pool Re since inception of the scheme.

Until 2015 Pool Re had never transferred risk into the reinsurance market. This changed on 1 March 2015 when Pool Re bought a single layer of retrocession, £1.8 billion excess of £500 million, from the external market. This layer was secured on a 3 year basis and cover is back-to-back with that provided by the scheme.

[Sources – Pool Re; Enoizi, 2015]

Box 4 – Flood Re

Flood Re is a joint industry/Government sponsored scheme to:

- enable flood cover to be affordable for those households at highest risk of flooding;
- increase availability and choice of insurers for customers;
- create a transitional measure to allow flood insurance to move towards risk-reflective pricing within 25 years;
- create a level playing field for new entrants and existing insurers in the UK home insurance market.

Flood Re was proposed by the UK insurance industry to the Government as an innovative, market based solution, to achieve the above objectives while minimising market distortion. It will provide support in the parts of the home insurance market that need it, which is likely to be around 2% of home insurance customers living in areas with the greatest risk of flooding. For the remaining 98%, the competitive home insurance market will continue to operate as it does today.

When Flood Re is in operation, customers will continue to buy their home insurance from an insurer as they do in the current market. However, insurers are able to reinsure (transfer) the flood risk element of the insurance to Flood Re at a fixed reinsurance premium based on the property's Council Tax Band. The premiums have been set sufficiently low to allow insurance to be affordable for homeowners however they are below the underlying 'technical risk cost'.

There is no requirement or limitation on insurers ceding business to Flood Re; such decisions will be based on their own commercial criteria. The approach should mean that there is no economic incentive for insurers to decline to quote for providing insurance coverage based on high flood risk (thus making coverage available for those properties). There should also be no economic incentive, based on a competitive market, for insurers to charge the customer more for the flood risk peril than the cost they will incur in ceding the flood risk peril to Flood Re (thus also making the coverage affordable to the customer).

Flood Re will be funded by:

- a £180m annual levy from all UK home insurers ("Levy 1");
- inwards reinsurance premiums received from insurers when transferring the flood risk of policies to Flood Re, based on the Council Tax band of the property; and
- an additional contribution or levy from all UK home insurers if needed ("Levy 2").

Until Flood Re starts operating as a reinsurer, ABI members are voluntarily continuing to meet their commitments to existing customers under the old Flood Insurance Statement of Principles agreement (which were set to expire in 2013).

[Source: Flood Re]

5.3 Stakeholders' views

This section explores in greater detail stakeholders' views on the role of government and the relevance of a public-private cyber-catastrophe reinsurance scheme. This section is largely informed by interviews with representatives of the insurance and reinsurance industry, though academics and other public and private sector interviews helped provide context.

Most respondents agreed that the UK government has a role to play in driving information sharing on cyber-risk. Some suggested that this should include sharing information on cyber threats through secure channels and anonymising data for modelling purposes.

All respondents agreed that a cyber-catastrophe would force significant government expenditure. Virtually all respondents believed that insurance could be a significant help in helping government manage this 'UK plc liability on the public sector balance sheet'.

However, this liability did not mean that a government reinsurer was essential. On the role of government cyber-catastrophe reinsurance, more than half of all the respondents had a view on the subject. A majority, in conversation, favoured a government-funded cyber-catastrophe reinsurer. However, thinking on the subject was not well-structured. Most respondents argued that a government-funded reinsurer would rapidly provide clarity and certainty to the market.

Among the minority who were against, most argued that it was too early to discuss the role of government suggesting that the insurance industry should first define its exposure to the risk and work out loss ratios. In addition, the minority argued that a wholly private sector approach was to be favoured if it could be made to work. Overall, respondents agreed, whatever their views on its desirability, that a government-funded cyber-catastrophe reinsurer was unlikely, at the very least until there was a significant cyber-catastrophe.

Most respondents felt that government promotion of a cyber-catastrophe reinsurance scheme would be highly valuable. Such a scheme could go a long way without government funding in starting to address cyber-risk. Respondents equally agreed that public-private cyber-catastrophe reinsurance scheme discussions should start now, before a cyber-catastrophe arises. Such a scheme would promote better definitions of cyber-catastrophe insurance; provide a forum for information exchange; place reinsurance cover as a group and explore other forms of covers such as ILS's. Respondents speculated that a final structure might be quite similar to Pool Re, or an extension of Pool Re.

6. RECOMMENDATION

This report finds that a cyber-catastrophe occurring today could potentially leave the UK exposed to catastrophic consequences. Cyber threats are real and there are significant gaps in existing insurance coverage. Risk mitigation through insurance and reinsurance seems to be below what would be necessary to mitigate cyber-risk at the scale of the country, given the £2 billion to £20 billion single event estimates. Cyber threats will be more rapidly addressed if cyber insurance grows more rapidly. The cyber insurance market will not grow quickly enough to address the threats without speeding up the supply of reinsurance.

A public-private reinsurance scheme would start to address the scale of risk management needed to mitigate cyber-catastrophes. The key points of such a scheme are that:

- the scheme should provide more standardised wordings linking cyber-catastrophe to the policies members write, and more standardised data collection for analytical purposes;
- the scheme should promote the use and evolution through learning of ICT security and risk management standards such as Cyber Essentials, ISO 27000, NIST, or CESG's 10 Steps;
- insurance regulators should strongly encourage membership of such a scheme by insurers providing cyber cover;
- members should jointly seek reinsurance for a cyber-catastrophe, including consideration of cyber-catastrophe linked securities;
- government should facilitate, but not underwrite, the scheme's reinsurance – government oversight could help the issuance of cyber-catastrophe linked bonds, while government permission to extend the Pool Re concept to cover cyber-catastrophe, by use of a separate scheme under the same management, would speed the scheme's growth;
- government and regulators should strongly encourage cyber insurance for essential services and critical national infrastructure including financial services, and incorporate cyber insurance in government procurement processes, e.g. requirement to purchase if unable to show appropriate management or retentions.

A public-private cyber-catastrophe reinsurance scheme would support UK cyber prosperity while adding clarity and certainty in the insurance market. As such, it could drive agreement on a standard cyber cover and wording, allowing the market to line up behind it in a unified fashion. It would support the provision of further private reinsurance capacity lacking in today's market. Down the line, it could help to remove exclusions from standard policies and to expand coverage to include business interruption, property damage and bodily injury. Such a scheme would almost certainly be set up in the aftermath of a black swan event. Such a scheme ought to include adequate requirements to support information sharing, such as:

- defining a requirement for government to provide anonymised data, subject to availability;
- defining a requirement for insurers to share information and data on events and associated losses within the scheme;
- establishing formal arrangements to share private data with the public sector.

A public-private catastrophe reinsurance scheme would only cover losses resulting from a cyber event beyond a pre-determined excess point. The scheme would in effect be a pool funded by the insurance industry, seeking its own further reinsurance and possibly issuing insurance linked securities such as a cyber-catastrophe bond for further cover. The UK government's role would be one of promotion and (possibly) a last resort insurer only in the event that industry retentions and the scheme's reserves have been exhausted. In all likelihood, the UK government would be a last resort insurer anyway but in this way it would benefit from a buffer much longer than the one it enjoys today.

Appendix 1 – Looking at the evidence: selected cyber attacks

Estonia – distributed denial of service attacks (DDoS)
2007 to 2008

In 2007, Estonia was hit by a three-week wave of massive cyber attacks in the form of DDoS which effectively disabled the websites of government ministries, political parties, newspapers, banks, and companies ultimately forcing the government and large banks to shut down Internet-based activities. The attacks were thought to be sponsored by Russia in reaction to Estonia's decision to remove a Soviet monument erected in 1947 in the capital, Tallinn. The media by and large described the attacks as 'cyber warfare' and mentioned Russia as a possible state-sponsor though the attackers were not clearly identified (see for example The Guardian, 2007; BBC, 2007). While the Estonian government immediately blamed Russia, EU and NATO officials were more cautious not to make any direct accusations against Russia. Russia always denied its involvement. Ultimately, evidence surfaced that the attacks came from hacktivists acting on their own initiative and combining experienced and novice hackers. One of the attackers, an ethnic Russian student residing in Estonia, was successfully traced and indicted in 2008. No subsequent arrests have been made to date (Richards, 2009).

***

Myanmar – DDoS attacks ahead of Burmese general election
2010

In 2010, a massive DDoS attack targeted the Burma's main Internet provider, the Ministry of Post and Telecommunication, disrupting the network and interfering with the majority of all incoming and outgoing traffic between October and November 2010. Significant speculation blamed the Burmese military government for a pre-emptive attack to disrupt the Internet just before the general election scheduled for 7 November, the first in 20 years. The Burmese government did not allow international observers and journalists to cover the polls. Further, it was known to restrict freedom of expression through Internet censorship (see Reporters Without Borders, n.d.; Sutherland, 2010; BBC, 2010).

***

Iran – Stuxnet attack against industrial control systems at Natanz nuclear plant
c. 2008/09 to 2012

In 2010, the existence of a cyber worm (a self-replicating computer virus) later called Stuxnet, was discovered at Natanz nuclear facility in Iran. Suspected to have been operating for over a year, Stuxnet aimed to physically destroy equipment by infecting the programmable-logic controllers (PLCs) run by computers. In this case, the worm caused centrifuges used to enrich uranium at the Natanz plant to slow down and fall at unprecedented rates for apparently unknown reasons (Zetter, 2014). Stuxnet was able to go undetected and to spread over local-area networks (i.e. closely connected computers) or through removable media (e.g. USB drive) (Cherry, 2012). Infections were not only found in Iran but also in Indonesia and elsewhere in Asia. Only a few infections were detected at sites in Europe and in the USA. At the time, Stuxnet was the largest piece of malicious software ever discovered (Cherry, 2012). Named the first 'cyber weapon', Stuxnet appeared to many experts to be "the product of a more sophisticated and expensive development process than any other piece of malware that has become publicly known" (Vanity Fair, 2011). Langner (2013: 20), an expert who reverse engineered the attack code of Stuxnet, argued that "the development of Stuxnet did require nation-state resources – especially for intelligence gathering, infiltration, and most of all for testing. […] the cyber weapon was way too complex to warrant any hope for successful operation without thorough testing." Writing for the New York Times, David Sanger reported, citing unnamed sources, that Stuxnet had been developed by the USA and Israel to undermine Iranian's nuclear programme (Sanger, 2012). Though the veracity of some details in Sanger's account has been questioned (see

for example Cherry, 2012), only Israel's intelligence agency's involvement seemed to have been acknowledged so far (see Stark, 2011).

***

Sony Pictures Entertainment Hack
2014

On 24 November 2014, Sony Pictures Entertainment (SPE) was made aware of a hack resulting in the release of confidential data including personal information about employees and their families, information about executive pay, copies of Sony films unreleased at the time and other information (see for example Robb, 2014). A group later identified as 'the Guardians of Peace' claimed to be behind the attack and demanded the cancellation of the planned release of the film 'The Interview' a comedy about a plot to assassinate North Korean leader Kim Jong-un. The group later also threatened to attack the movie theatres who would show the movie. SPE first looked at the hack as an IT issue before acknowledging a week later that a large amount of confidential data had been stolen (Robb, 2014).

Mandiant, a cyber security firm hired to investigate the attack found that it was well planned and probably carried out by an 'organized group' with the purpose of both destroying property and releasing confidential information to the public (Reuters, 2014; Robb, 2014). A North Korea spokesman was quoted by KCNA earlier in the year about the release of the movie calling it 'an act of terrorism and war' which could not be tolerated (BBC, 2014). Speculation about North Korea's possible involvement in the cyber attack rose but the government denied its involvement (BBC, 2014). In an interview to CNN, President Obama called it an "act of cyber vandalism" rather than 'act of war' which turned out to be "very costly, very expensive". He added that the US "take it very seriously" and "will respond proportionately" (CNN, 2014). When North Korea's Internet experienced unusual connectivity issues and failures a few days later, questions were raised as to whether this was part of the 'US response'. The US government did not comment on it (The Washington Post, 2014). On 2 January 2015, the US government announced new financial sanctions against 10 North Korean government officials and three organisations, in retaliation for the country's alleged role in hacking Sony Pictures' systems (Roberts, 2015). The North Korean government denied once more its involvement in the attack (Siddique, 2015).

On 30 April 2015, Sony disclosed its consolidated financial results forecast for the fiscal year ended 31 March 2015 which included an estimated cost of US$41 million in relation to investigation and remediation costs following the cyber attack against SPE's network and IT infrastructure (Sony, 2015 (a): 5). In its fiscal third quarter report, Sony stated: "Sony believes that the impact of the cyber attack on its consolidated results for the fiscal year will not be material" (Sony, 2015 (b): 10). The company senior management expects to recover a significant portion of the costs associated with leaks of unreleased movies and disruption to their IT systems thanks to cyber insurance. The full cost of the attack remains difficult to assess past the 'clean up' costs in particular in relation to business interruption and legal costs (Peterson, 2014).

***

USA – cyber espionage by Chinese military hackers
2006 to 2014

In May 2014 a grand jury in the Western District of Pennsylvania (WDPA) indicted five Chinese military hackers for computer hacking, economic espionage and other offenses directed at six American victims in the U.S. nuclear power, metals and solar products industries (US Department of Justice, 2014). The attacks are estimated to have been ongoing since 2006 and to involve spear phishing to gain access. The hackers were officers in Unit 61398 of the Third Department of the Chinese People's Liberation Army, suggesting state involvement in cyber espionage. China denied involvement reacted to the indictment by suspending high-level cyber talks with the United States and the activities of the

corresponding US-China Cyber Working Group. (Nakashima & Wan, 2014; Ministry of Foreign Affairs of the People's Republic of China, 2014)

***

Germany – steel mill cyber attack
2014

In December 2014, an IT security report published by Germany's Federal Office for Information Security revealed that an unnamed steel plant had suffered a cyber attack (BSI, 2014). The attack resulted in significant physical damage due to critical process components becoming unregulated and a blast furnace was prevented from shutting down normally, thus leaving it in an undefined condition which caused damage to the whole system. The attack was termed an advanced persistent threat (APT) attack involving the use of spear phishing and social engineering. The report mentioned that the attackers were likely to have advanced technical knowledge of not only conventional IT security, but also industrial control systems (ICS) and production processes. The German report was the first source to report the attack though it did not provide much details on either the victim, any evidence on the attacker or their capabilities (Kovacs, 2014; BBC, 2014; Lee *et al*., 2014).

Appendix 2 – Comparison of terrorism risk insurance programmes in selected countries

	Australia	France	Germany	UK	USA
Facility	Australian Reinsurance Pool Corporation (ARPC)	Gestion de l'assurance et de la Réassurance des Risques Attentats et Actes de Terrorisme (GAREAT) Caisse Centrale de Réassurance (CCR)	Extremus Versicherungs-AG	Pool Reinsurance Company Limited (Pool Re)	Terrorism Risk Insurance Programme (TRIP) [sources: Hartwig & Wilkinson, 2015; Torregrosa *et al*., 2015]
Status	Established in 2003. Renewed in 2012 for three years. Decision to be made in 2015 regarding its continuation.	GAREAT established in December 2001, operational on 1 January 2002. CCR established in 1946.	Set up on 3 September 2002, operation in November 2002. Federal guarantee renewed in 2013 until end of 2015 when it will be subject to review.	Established in 1993 after the introduction of the Reinsurance Act 1993. Permanent regime revised periodically. Last revision in 2014.	Established in 2002 under the Terrorism Risk Insurance Act. Last extended in 2015, ensuring continuity until December 2020.
Purpose	Set up so that terrorism insurance could be offered with standard cover. Cover capped at $10 bn liability	CCR provides unlimited cover. GAREAT was established after 9/11 to prove coverage for large scale events (insured value in excess of €6 m)	Public company set up to facilitate the provision of terrorism insurance. Initiative of German Insurance Association with German reinsurance companies as shareholders.	Set up to facilitate the coverage of terrorism risk in commercial property insurance following IRA bombings in early 1990s.	Set up to overcome problems with availability and affordability of terrorism insurance following 9/11 and to overcome disruption in the market.
Coverage	Commercial risk; industrial risks; construction risks and interruption to farming.	All lines of property and business interruption other than transport, aviation hull and marine hull.		Pool Re covers losses resulting from damage to commercial property and business interruption.	Requires certified act of terrorism. Only claims occurring in certain property/casualty commercial lines of insurance are included in the calculations of insured losses under TRIA.

	Australia	France	Germany	UK	USA
Status of cyber-risk	Cyber crime excluded.	Unclear – possibly included by default (i.e. lack of defined exclusion)	Cyber attacks excluded.	Computer hacking, virus and denial of services are excluded.	Depends if cyber-risk is included or excluded in individual contract.
Layers of cover	Three layers: • industry retention ($375m); • ARPC pool which includes retrocession programme ($3 bn); • Commonwealth guarantee ($10 bn).	Six layers: €500 m industry annual contribution; €500 m from reinsurance; €500 m from international reinsurance; €500 m; €420 million in excess of the €2 bn already provided; then CCR provides unlimited protection in excess of the € 2,420 m provided, backed by the French State guarantee.	Two layers: • €2 bn provided by international market including international reinsurance; • €8 bn provided by German Government.	Three layers: • Industry retention amounts (based upon a proportion of the industry wide aggregate of £100 m per event and £200 m annual aggregate) • Pool RE covers up to the full amount of the fund (circa £5.5 bn) • UK government indemnity up to 100% of the claims above the fund value.	Trigger event phased from $100 m to £200 m insured losses by 2020. Federal assistance after deductibles are paid, of 80% of insured losses (remaining 20% co-payed by individual insurer) up to $100 bn losses. Aggregated industry wide retention between deductibles and co-payments will total $37.5 bn by 2020.
Government role	Third layer of cover once other two previous are exhausted. Capped liability at $10bn. Government received dividends in 2013	Unlimited cover with state guarantee with CCR once previous five layers of cover (€ 2,420 m) have been exhausted). CCR receives a premium.	Second layer of cover once first is exhausted.	Government acts as an insurer of last resort. Has never been asked to cover claims so far. Government receives a premium for coverage.	Liability capped at $100bn, inclusive of both insurer and government participation. No federal assistance below $200 m in insured losses.

[Source: OECD, 2015 unless specified otherwise]

Appendix 3 – Interview template (insurance)

1. Could you tell me about your role and how it relates to insurance and emerging risks?
2. How do you or does your organisation treat cyber-risk (or insurance)?
3. What do you think constitutes cyber-risk?
4. How would you define cyber-terrorism? How is cyber-terrorism different from other cyber threats?
5. What are the key features of cyber-terrorism to be taken into account from an insurance perspective?
6. What cyber-risks can be covered by insurance? E.g. business interruption, damage to property, intellectual property theft, data theft.
7. How do you/how would you assess exposure to cyber-risk?
8. What restrictions generally (or would) apply when underwriting cyber-risk?
9. What factors influence the price (premium) of cyber insurance coverage?
10. Is there demand for cyber-risk insurance products? From what type of clients? For what type of risks?
11. What is the biggest obstacle to a cyber insurance market?
12. What is the biggest obstacle to a cyber-catastrophe insurance market?
13. What are the opportunities and barriers to insurance product development for cyber-catastrophe?
14. How would you handle a cyber-terrorism claim, e.g. does an attacking state need to be identified, or would you accept the adjudication of a government reinsurer itself?
15. How do insurance companies (or how does your organisation) currently assess their exposure to cyber catastrophic risk? (e.g. in the event of multiple pay-outs should such risks materialise suddenly for an important portion of policy holders)
16. Is existing cyber terrorism reinsurance sufficient? i.e. is wider cyber reinsurance needed?
17. What would the benefits of having a public private cyber reinsurance be …
    … to insurers?
    … to policy holders (e.g. companies)?
    … to government(s)?
    … to other relevant stakeholders?
18. How could public-private cyber-catastrophe reinsurance scheme work and cover insurers?
19. What would be the benefits of such public-private reinsurance? and to whom?
20. If a public-private partnership is not possible, are there other possible approaches or relevant financial models which should be explored? (e.g. insurance-linked securities (ILS))
21. What issues does cyber-risk present for insurance companies in terms of capital adequacy regulatory requirements (e.g. Solvency II)?
22. How would cyber-catastrophe reinsurance help to address capital adequacy regulatory requirements?
23. Should cyber-catastrophe reinsurance be national, regional or international?

Appendix 4 – Acknowledgements

We received enthusiastic cooperation from everyone involved in this project. We would like to thank all the people who agreed to semi-structured interviews and who contributed to events. Without implying any responsibility for this report and its conclusions, nor any endorsement of our work by them or their organisations, people working at the following organisations were particularly helpful to us and we thank them:

2iC
Association of British Insurers
ACE
ACORD
Aegis
AIR
Airmic
Antares Underwriting
Aon Benfield
APM Group
Ariel Re Bermuda
Ark Syndicate Management
Ascot Syndicate
APM Group
Axis Specialty London
Bank of England
Barclays
Beazley
BMS Group
BNY Mellon
Brechin Tindal Oatts Solicitors
Brighton Rock Insurance
Brit Insurance
British Business Federation Authority
BT
Cabinet Office
Canopius
Capsicum Re
Catlin Group
Centre for Economics and Business Research (CEBR)
Centre for the Study of Financial Innovation (CSFI)
Citi
City of London Corporation
City of London Police
Countermeasures Consulting
Cyberterrorism Project (Swansea University)
Department for Business Innovation and Skills (BIS)
Defence Science and Technology Laboratory (Dstl)
Endava
Falanx Group
FCA
Fitch Ratings
Flood Re
Guardtime
Guildhall Corporate Advisers
Hardy Underwriting (CNA)
Hiscox
HM Treasury
HP
HSBC
Information Security Forum
Lighthill Risk Network
Lloyd's
London Market Group
Marsh
Microsoft
Miller Insurance
Munich Re
National Audit Office
Oasis
OECD
Oxford Martin School Global Cyber Security Capacity Centre
Panaseer
Philippa Ross & Co
Pool Re
RFIB
Risk Management Solutions (RMS)
Security Forward
Scor UK
Swiss Re
Talbot Syndicate
TechCityUK
Technium Global Limited

Templar Executives
TheCityUK
ThinkingSafe
Tokio Millennium Reinsurance
Tori Global
Torus
UK Government Actuary's Department
Validus Re
VocaLink
Willis

Appendix 5 – Bibliography

American Institute For Chartered Property Casualty Underwriters (CPCU). “Quota-share insurance.” In *Types of Reinsurance and Reinsurance Program Design*, 2.5 to 2.8. American Institute For Chartered Property Casualty Underwriters, 2013.

Aon Risk Solutions. “Cyber Risk and the Captive Market: A Match Made in the Cloud?”. Aon. 2014

Association of British Insurers (ABI). “Cyber Insurance.” *Association of British Insurers.* 19 March 2015. (accessed 20 July 2015).

Bank of England Prudential Regulatory Authority (PRA). General Insurance Stress Test 2015: Scenario Specification, Guidelines and Instructions. Scenario Specification, London, UK: Bank of England, 2015, 38 pages.

BBC. “Burma hit by massive net attack ahead of election.” 4 November 2010.

—. “Hack attack causes 'massive damage' at steel works.” 22 December 2014.

—. “Estonia hit by ‘Moscow cyber war’.” 17 May 2007.

—. “North Korea denies 'righteous' hack attack on Sony.” 7 December 2014.

—. “North Korea threatens war on US over Kim Jong-un movie.” 26 June 2014.

Betterley, Richard. *The Betterley Report - Cyber/Privacy Insurance Market Survey 2015.* Survey, Sterling, USA: Betterley Risk Consultants, Inc, 2015, 17 pages.

Biener, Christian, Martin Eling, and Jan Hendrik Wirfs. *Insurability of Cyber risk: An Empirical Analysis.* Working Papers on Risk Management and Insurance no 151, Institute of Insurance Economics, University of St Gallen, University of St Gallen, 2015, 32 pages.

BIS. “Die Lage der IT-Sicherheit in Deutschland 2014.” 2014.

Cabinet Office. *National Risk Register of Civil Emergencies. 2015 edition.* London, UK: Cabinet Office, 2015, 57 pages.

Cabinet Office. *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world.* Cabinet Office, 2011.

Cambridge Centre for Risk Studies (CCRS). “Cyber catastrophe Defining a Risk Test Scenario for managing the business risks posed by cyber threats.” 16 December 2014.

CEA. *Reducing the Social and Economic Impact of Climate Change and Natural Catastrophes - Insurance Solutions and Public-Private Partnerships.* Brussels: CEA, 2007, 47 pages.

Center for Strategic and International Studies. *Net Losses: Estimating the Global Cost of Cybercrime - Economic impact of cybercrime II.* McAfee, 2014, 24 pages.

Centre for the Study of Financial Innovation (CSFI). *Insurance Banana Skins 2015.* CSFI, 2015.

Cherry, Steven. “Stuxnet: Leaks or Lies?” *IEEE Spectrum.* IEEE, 4 September 2012.

CNN. “Obama: North Korea's hack not war, but 'cybervandalism'.” 21 December 2014.

Comité Européen des Assurances (CEA). *Insurance and reinsurance of data losses caused by computer viruses.* Briefing note, CEA, 2003, 10 pages.

Conway, Maura. “Cyberterrorism: The Story So Far.” *Journal of Information Warfare* 2, no. 2 (2003): 33-42.

CRO Forum. *Cyber resilience – The cyber risk challenge and the role of insurance.* CRO Forum, 2014.

Denning, Dorothy E. "Chapter 8: Activism, Hacktivism and Cyberterrorism: the Internet as a Tool for Influencing Foreign Policy." In *Networks and Netwars: The Future of Terror, Crime, and Militancy* , by John Arquilla and David Ronfeldt, 239-288. RAND Corporation, 2001.

—. "Statement on Terrorist Threats to the United States." *US Congress 2000 Hearings.* Federation of American Scientists - Intelligence Resource Programme, 23 May 2000. 1-5.

Detica & Cabinet Office. *The Cost of Cyber Crime.* Industry report, London: Cabinet Office, 2011, 1-28.

Enoizi, Julian. "2015 Pool Re AGM Presentation." London: Pool Re, June 2015.

European Network and Information Security Agency (ENISA). *Incentives and barriers of the cyber insurance market in Europe.* Heraklion, Greece: ENISA, 2012, 45 pages.

FBI. "Five Chinese Military Hackers Charged with Cyber Espionage Against U.S." 19 May 2014.

GCHQ & Cert-UK. *Common Cyber Attacks: Reducing The Impact.* London: UK Government, 2015, 17 pages.

Gibbs, Samuel. "Eugene Kaspersky: major cyberterrorist attack is only matter of time." *The Guardian.* 1 May 2014.

Gracie, Andrew. "Managing cyber risk – the global banking perspective." London: Bank of England, 10 June 2014. 5 pages.

Guy Carpenter. "Guy Carpenter Mid-Year Review Assesses Key Industry Trends". News release. 14 July 2014. 3 pages.

Hartwig, Robert P., and Claire Wilkinson. "Terrorism Risk Insurance Program: Renewed and Restructured." Insurance Information Institute, 2015.

Hartwig, Robert, and Claire Wilkinson. *Cyber risks: The Growing Threat.* Insurance Information Institute, 2014, 27 pages.

HM Government. *Cyber Essentials.* (accessed 20 July 2015).

HUB International. "Cyber Insurance." *CTMA.* (accessed 20 July 2015).

ISO. "ISO/IEC 27001 - Information security management." *ISO.* (accessed 20 July 2015).

—. "ISO/IEC 27032:2012 - Information technology - Security techniques -Guidelines." *ISO.* 2012. (accessed 20 July 2015).

Janczewski, Lech J., and Andrew M. Colarick. *Cyber Warfare and Cyber Terrorism.* Information Science Reference, IGI Global, 2008.

Kaspersky Lab. *Equation Group: Questions and Answers.* FAQ, Kaspersky Lab, 2015, 43 pages.

Kovacs, Eduard. "Cyberattack on German Steel Plant Caused Significant Damage: Report." *Security Week.* 18 December 2014.

KPMG. "Senior security heads don't trust cyber insurance products ." KPMG, 1 May 2015.

Langner, Ralph. *To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve.* Technical report, Langner, 2013, 36 pages.

Lee, Robert M., Michael J. Assante, and Tim Conway. *German Steel Mill Cyber Attack.* Case study report, ICS, 2014, 15 pages.

Liès, Michel. "How Do You Insure Against Cybercrime?". *The Wall Street Journal*, 21 April 2015.

Lloyd's & CCRS. *Business Blackout: The insurance implications of a cyber attack on the US power grid.* Emerging Risk Report, London, UK: Lloyd's, 2015, 65 pages.

LMG & BCG. *London Matters: The competitive position of the London Insurance Market .* Industry report, LMG & BCG, 2014, 54 pages.

Mainelli, Michael. "Learn From Insurance: Cyber Bore", *Journal of Risk Finance*, Volume 14, Number 1, Emerald Group Publishing (January 2013), pages 100-102.

Mainelli, Michael. "Cyber's Empty Space", *Financial World*, IFS School of Finance (December 2012), page 39.

Mandiant. *M-Trends 2015: a view from the frontline.* Threat report, Mandiant, FireEye, 2015, 24 pages.

Marsh. "Benchmarking Trends: As Cyber Concerns Broaden, Insurance Purchases Rise." Risk Management Research, 2015, 4 pages.

Marsh & Cabinet Office. "UK cyber security: the role of insurance in managing and mitigating the risk." London, 2015, 32 pages.

Marsh. *Global Insurance Market Quarterly Briefing.* Global Insurance Market Quarterly Briefing, Marsh, 2015, 4 pages.

Marsh. *UK and Ireland 2014 Cyber risk Survey Report.* Survey, Marsh, 2014.

Ministry of Foreign Affairs of the People's Republic of China. "China Reacts Strongly to US Announcement of Indictment Against Chinese Personnel." 19 May 2014.

Mole, Alastair. "Maximising value from emerging cyber reinsurance." *The Independent Broker*, September 2014.

Nakashima, Ellen, and William Wan. "U.S. announces first charges against foreign country in connection with cyberspying." *The Washington Post.* 19 May 2014.

National Academy of Sciences. *Severe Space Weather Events - Understanding Societal and Economic Impacts .* Workshop report, Washington DC: National Academy of Sciences, 2008, 145 pages.

National Institute of Standards and Technology (NIST). *Framework for Improving Critical Infrastructure Cybersecurity.* NIST, 2014, 39 pages.

NATO. "Wales Summit Declaration." NATO, 5 September 2014.

"NMA 2914." *Equinox Underwriting.* 25 January 2001. (accessed 20 July 2015).

Obama, Barack. "Improving Critical Infrastructure Cybersecurity." Executive Order. The White House, Office of the Press Secretary, 12 February 2013.

OECD. *National Terrorism Risk Insurance Programmes of OECD Countries with Government Participation - Main Features.* Comparative table, OECD, 2015, 8 pages.

Oxford Economics & CPNI. *Cyber attacks: Effects on UK Companies.* Research report, Oxford Economics, 2014, 76 pages.

Papanikolaou, Ioannnis, and Marie Gemma Dequae. "Definition of Catastrophe." Presentation. Frankfurt, 28 April 2015. 25 pages.

Peterson, Andrea. "Why it's so hard to calculate the cost of the Sony Pictures hack." *The Washington Post.* 5 December 2014.

Ponemon Institute & IBM. *2015 Cost of Data Breach Study: United Kingdom.* Research report, Ponemon Institute, 2015, 21 pages.

Pool Re. *Pool Re.* (accessed 20 July 2015).

Powers, Michael R. *Acts of God and Man.* Columbia Business School Publishing, 2012.

RAND Institute for Civil Justice. *Compensating the Victims of 9/11.* Research brief, RAND, 2004, 3 pages.

Reactions. "Government cyber backstops needed: Lloyd's". *Reactions*. 13 July 2015

Reporters Without Borders. "Internet Enemies - Burma." *Reporters Without Borders.* (accessed 20 July 2015).

Reuters. "Hacking Experts Call Sony Cyber Attack 'Unparalleled And Well Planned Crime'". 7 December 2014.

Richards, Jason. "Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security." *International Affairs Review*, 2009.

Robb, David. "Sony Hack: A Timeline." *Deadline .* 22 December 2014.

Roberts, Dan. "Obama imposes new sanctions against North Korea in response to Sony hack." *The Guardian.* 2 January 2015.

Ruffle, S.J., *et al*. *Sybil Logic Bomb Cyber catastrophe Scenario .* Cambridge, UK: CCRS, 2014, 41 pages.

Russell. "Insuring the intangible - Intangible Risks Roundtable." *Reactions*, February 2014: 37-40.

Sanger, David E. "Obama Order Sped Up Wave of Cyberattacks Against Iran." *The New York Times.* 1 June 2012.

Siddique, Haroon. "North Korea responds with fury to US sanctions over Sony Pictures hack." *The Guardian.* 5 January 2015.

Sony. "Consolidated Financial Results for the Fiscal Year Ended March 31, 2015." Tokyo: Sony, 30 April 2015.

—. "Consolidated Financial Results for the Third Quarter Ended December 31, 2014 and Revision of Consolidated Forecast for the Fiscal Year ending March 31, 2015." Tokyo: Sony, 4 February 2015.

Standard & Poor's. *Looking before they leap: US Insurers dip their toes in the Cyber Risk Pool.* Standard & Poor's, 2015, 5 pages.

Stark, Holger. "Mossad's Miracle Weapon: Stuxnet Virus Opens New Era of Cyber War." *Spiegel online.* 8 August 2011.

Statista. "Share of U.S. companies with standalone cyber insurance 2013-2014, by industry." *Statista.* 2015. (accessed 20 July 2015).

Sutherland, JJ. "Myanmar's Internet Under Cyberattack." *NPR.* 4 November 2010.

Swiss Re. "Natural catastrophes and man-made disasters in 2013." *Sigma*, 2014: 50 pages.

Tendulkar, Rohini. *Cyber crime, securities markets and systemic risk.* Working Paper, IOSCO & World Federation of Exchanges, 2013, 58 pages.

The Guardian. "Russia accused of unleashing cyberwar to disable Estonia." 17 May 2007.

The United States Department of Justice. "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage." 19 May 2014.

The Washington Post. "North Korea's Internet outage was likely the work of hacktivists — but not the ones you might think." 23 December 2014.

Theohary, Catherine A., and John W. Rollins. *Cyberwarfare and Cyberterrorism: In Brief.* Congressional Research Services, 2015, 1-12.

Torregrosa, David, Perry Beider, and Susan Willie. "Federal Reinsurance for Terrorism Risk in 2015 and Beyond." Working paper, Congressional Budget Office, 2015, 38 pages.

UK Department for Business, Innovation and Skills (BIS). *2014 Information Security Breaches Survey.* Survey , BIS, 2014, 20 pages.

—. "Cyber Essentials Scheme - Summary." London: BIS, June 2014. 10 pages.

UK Government. "Cyber security boost for UK firms." London: UK Government , 16 January 2015.

—. "Guidance - Cyber Essentials Scheme Overview." *GOV.UK.* 3 February 2015. (accessed 20 July 2015).

—. "UK Cyber Security Strategy: statement on progress 3 years on." London: GOV.UK, 11 December 2014.

Vanity Fair. "Stuxnet Worm: A Declaration of Cyber War", April 2011.

Weimann, Gabriel. *Cyberterrorism: how real is the threat?* Special report, Washington DC: United States Institute of Peace (USIP), 2004, 11 pages.

World Economic Forum. *The Global Risks report 2015.* World Economic Forum, 2015, 60 pages.

Willis, Finex Global, "Cyber risk: Security, Network and Privacy" (brochure), 2014.

Yasuda, Yosuke. *Gearing up for cyber risk.* Swiss Re, 2014, 18 pages.

Zetter, Kim. "An Unprecedented Look at Stuxnet, the World's First Digital Weapon." *Wired.* 11 March 2014.

—. "A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever." *Wired*, 1 August 2015.

www.longfinance.net

In collaboration with:

http://apmg-cyber.com/

Produced by:

www.zyen.com