An overview of the cyber insurance industry: Challenges for insurers and insureds in quantifying and mitigating cyber risk

Michael Payne

Technical Report
RHUL–ISG–2017–9
10 February 2017
An Overview of the Cyber Insurance Industry: Challenges for Insurers and Insureds in Quantifying and Mitigating Cyber Risk

Supervisor: Peter Komisarczuk

Submitted as part of the requirements for the award of the MSc in Information Security at Royal Holloway, University of London.

I declare that this assignment is all my own work and that I have acknowledged all quotations from published or unpublished work of other people. I also declare that I have read the statements on plagiarism in Section 1 of the Regulations Governing Examination and Assessment Offences, and in accordance with these regulations I submit this project report as my own work.

Signature: [Signature]

Date: 23 August 2016
Abstract

The purpose of this study is to present the cyber risks facing all organisations, how they treat these risks, and the options available when risks are transferred. An overview of the cyber insurance industry is then laid out providing a background into the development of cyber cover, common types of cover available, and how cyber risks are underwritten. The specific challenges facing insurers include a lack of historical data, accumulation risks, data sharing and quantification of risks, and how risks are managed. Organisations should treat cyber risk as an operational risk and one which is central to business strategy and objectives. Not all risk can be retained so potential insureds need to navigate an array of insurance products which may include certain cyber risks, but not others. Legal developments also present certain challenges for both insurers and insureds. The study concludes with a future outlook for the cyber insurance industry.
Acknowledgements

To my amazing and lovely wife, Marie, who has been so supportive throughout my studies and change in career.
Abstract ........................................................................................................................................... 2
Acknowledgements .......................................................................................................................... 3
Table of Contents ............................................................................................................................. 4
List of Figures .................................................................................................................................... 6
List of Tables ...................................................................................................................................... 6
List of Abbreviations and Acronyms ................................................................................................. 7
Introduction ......................................................................................................................................... 9

1. The Cyber Risk Landscape ............................................................................................................. 12
   1.1. Cyber Attacks .......................................................................................................................... 12

2. Operational Risk ............................................................................................................................. 18
   2.1. Risk Management ...................................................................................................................... 18
   2.2. Cyber Risk ................................................................................................................................. 26

3. Overview of Insurance .................................................................................................................... 30
   3.1. Insurability Criteria .................................................................................................................... 32

4. Cyber Insurance .............................................................................................................................. 34
   4.1. Growth of Cyber Insurance ....................................................................................................... 34
   4.2. Cyber Insurability Criteria ......................................................................................................... 35

5. Types of Cyber Cover ...................................................................................................................... 41
   5.1. Add-On Services ....................................................................................................................... 44
       5.1.1. Ex-Ante Services .............................................................................................................. 44
       5.1.2. Ex-Post Services .............................................................................................................. 44

6. Challenges Facing Insurers ............................................................................................................ 46
   6.1. Legislative Drivers ..................................................................................................................... 46
   6.2. Lack of Data .............................................................................................................................. 50
   6.3. Data Sharing Schemes ............................................................................................................. 52
   6.4. Implicit Cover or Silent Exposure ............................................................................................. 53
   6.5. Accumulation Risk ................................................................................................................... 56
   6.6. Capital Requirements ............................................................................................................... 58
   6.7. Diversification of Risk ............................................................................................................. 60

7. Challenges Facing Insureds ............................................................................................................. 63
   7.1. How is Cyber Risk Treated in the Organisation? ...................................................................... 64
   7.2. Risk Retention, Risk Mitigation or Risk Transfer ...................................................................... 65
   7.3. Lack of Standardised Cover ....................................................................................................... 69
   7.4. Attribution and Exclusions ....................................................................................................... 74
   7.5. Legislative Drivers and Legal Risks ......................................................................................... 80
   7.6. The SME Challenge ................................................................................................................. 82

8. Future Outlook ................................................................................................................................ 85
Conclusion.......................................................................................................................... 89

Appendices ................................................................................................................................92
I. Interviewees and Contributors ..................................................................................................92
II. Interview Questionnaire ..........................................................................................................93
III. Interview Transcripts ...............................................................................................................95
   Interview 1. Matthew Cullen, Association of British Insurers, 12 July 2016 .........................95
   Interview 2. Andrew Maher, Beazley, 30 June 2016 ..............................................................97
   Interview 5. James Burns, CFC Insurance, 20 July 2016 ......................................................101
   Interview 6. Matthew Webb, Hiscox, 29 June 2016 ............................................................103
   Interview 7. Andrew Ninian, Investment Association, 21 June 2016 .................................104
   Interview 8. John Golifer / Laura Hayter, Investor Relations Society, 5 July 2016 ..........105
   Interview 10. Chris Storer, Munich Re, Corporate Services Partner, 8 July 2016 ..........108
   Interview 11. Brian Barnier, ValueBridge Advisors, 8 August 2016 .................................109
   Interview 12. Scott Ernst, Wells Fargo Insurance Services Inc., 8 August 2016 ............110
   Interview 13. Peter Armstrong, Willis Towers Watson, 26 July 2016 ..............................112
IV. Categories of Cyber Risk .....................................................................................................115

Bibliography .......................................................................................................................... 116
List of Figures

Figure 1 - The Growth of the Cyber Risk Landscape .......................................................... 15
Figure 2 - Information Security Risk Management Process ................................................ 20
Figure 3 - Risk Treatment Options ......................................................................................... 22
Figure 4 - Risk Treatment Heat Map ....................................................................................... 23
Figure 5 - Risk Treatment Heat Map with Strategy Options .................................................. 24
Figure 6 - The Insurance Chain ............................................................................................... 30
Figure 7 - Assessment of Cyber Risk ...................................................................................... 40
Figure 8 - The Top 10 Most Common Categories of Cyber Loss Cover Across 26 Different
           Categories .................................................................................................................. 43
Figure 9 - Insurability of Risks ............................................................................................... 72
Figure 10 - Cyber Risks and Cover Provided by Traditional Lines of Insurance ................ 76
Figure 11 - Risk Profile for SMEs ........................................................................................... 84

List of Tables

Table 1 - ENISA Threat Landscape ....................................................................................... 16
Table 2 - Berliner Insurability Criteria .................................................................................. 32
Table 3 - Categories of First and Third-Party Cover ............................................................... 41
Table 4 - Cyber Insurance Penetration Rate ......................................................................... 66
Table 5 - Exclusions and Limits of Cover in Traditional Insurance Lines ............................. 78
Table 6 - Interviewees and Contributors .............................................................................. 92
Table 7 - Categories of Cyber Risk ....................................................................................... 115
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABI</td>
<td>Association of British Insurers</td>
</tr>
<tr>
<td>IoT</td>
<td>Internet of Things</td>
</tr>
<tr>
<td>BEC</td>
<td>Business Email Compromise scam (sometimes referred to as CEO Fraud)</td>
</tr>
<tr>
<td>BIBA</td>
<td>British Insurance Brokers Association</td>
</tr>
<tr>
<td>CBI</td>
<td>Contingent Business Interruption</td>
</tr>
<tr>
<td>CCRS</td>
<td>Cambridge Centre for Risk Studies</td>
</tr>
<tr>
<td>CERT-UK</td>
<td>UK National Computer Emergency Response Team</td>
</tr>
<tr>
<td>CGL</td>
<td>Commercial General Liability Insurance Cover</td>
</tr>
<tr>
<td>CISP</td>
<td>Cyber-security Information Sharing Partnership</td>
</tr>
<tr>
<td>COSO</td>
<td>Committee of Sponsoring Organisations of the Treadway Commission</td>
</tr>
<tr>
<td>CSIRT</td>
<td>Computer Security Incident Response Team</td>
</tr>
<tr>
<td>CL380</td>
<td>Institute Cyber Attack Exclusion Clause</td>
</tr>
<tr>
<td>CY</td>
<td>Cyber Security Data and Privacy Breach (Lloyd’s risk code)</td>
</tr>
<tr>
<td>CZ</td>
<td>Cyber Security Property Damage (Lloyd’s risk code)</td>
</tr>
<tr>
<td>D&amp;O</td>
<td>Directors and Officers Insurance Cover</td>
</tr>
<tr>
<td>E&amp;O</td>
<td>Errors and Omissions Insurance Cover (also known as Professional Liability)</td>
</tr>
<tr>
<td>EBITDA</td>
<td>Earnings Before Interest Tax Depreciation and Amortization</td>
</tr>
<tr>
<td>ERM</td>
<td>Enterprise Risk Management</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>FERPA</td>
<td>Family Educational Rights and Privacy Act</td>
</tr>
<tr>
<td>FISMA</td>
<td>Federal Information Security Modernization Act of 2014</td>
</tr>
<tr>
<td>FOIA</td>
<td>Freedom of Information Act</td>
</tr>
<tr>
<td>FS-ISAC</td>
<td>Financial Services Information Sharing and Analysis Centre</td>
</tr>
<tr>
<td>GDPR</td>
<td>General Data Protection Regulation</td>
</tr>
<tr>
<td>GLBA</td>
<td>Gramm Leach Bliley Act</td>
</tr>
<tr>
<td>GWP</td>
<td>Global Written Premium</td>
</tr>
<tr>
<td>HIPAA</td>
<td>Health Insurance Portability and Accountability Act</td>
</tr>
<tr>
<td>HITECH</td>
<td>Health Information Technology for Economic and Clinical Health Act</td>
</tr>
<tr>
<td>IBNR</td>
<td>Incurred But Not Reported claims</td>
</tr>
<tr>
<td>ICO</td>
<td>Information Commissioner’s Office</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communications Technology</td>
</tr>
<tr>
<td>ILS</td>
<td>Insurance Linked Securities</td>
</tr>
<tr>
<td>ISO</td>
<td>International Standards Organisation</td>
</tr>
<tr>
<td>ISACA</td>
<td>Information Systems Audit and Control Association</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>KSI</td>
<td>Keyless Signature Infrastructure</td>
</tr>
<tr>
<td>LMA</td>
<td>Lloyd’s Market Association</td>
</tr>
<tr>
<td>NAIC</td>
<td>National Association of Insurance Commissioners</td>
</tr>
<tr>
<td>NCSC</td>
<td>National Cyber Security Centre (UK)</td>
</tr>
<tr>
<td>NIS</td>
<td>Network and Information Security Directive</td>
</tr>
<tr>
<td>NIST</td>
<td>The National Institute of Standards and Technology</td>
</tr>
<tr>
<td>OCR</td>
<td>Office of Civil Rights</td>
</tr>
<tr>
<td>OCTAVE</td>
<td>Operationally Critical Threat, Asset, and Vulnerability Evaluation</td>
</tr>
<tr>
<td>ORSA</td>
<td>Own Report on Self-Assessment</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>OT</td>
<td>Operational Technology</td>
</tr>
<tr>
<td>P&amp;C</td>
<td>Property and Casualty Insurance Cover</td>
</tr>
<tr>
<td>PCI DSS</td>
<td>Payment Card Industry Data Security Standard</td>
</tr>
<tr>
<td>PFI</td>
<td>Personal Financial Information</td>
</tr>
<tr>
<td>PHI</td>
<td>Personal Health Information</td>
</tr>
<tr>
<td>PII</td>
<td>Personally Identifiable Information</td>
</tr>
<tr>
<td>PML</td>
<td>Probable Maximum Loss</td>
</tr>
<tr>
<td>RBC</td>
<td>Risk Based Capacity</td>
</tr>
<tr>
<td>RCA</td>
<td>Root Cause Analysis</td>
</tr>
<tr>
<td>RMS</td>
<td>Risk Management Solutions, Inc.</td>
</tr>
<tr>
<td>SCADA</td>
<td>Supervisory Control and Data Acquisition</td>
</tr>
<tr>
<td>SEI</td>
<td>Software Engineering Institute, Carnegie Mellon University</td>
</tr>
<tr>
<td>SOX</td>
<td>Sarbanes Oxley Act 2002</td>
</tr>
<tr>
<td>TCO</td>
<td>Total Cost of Risk</td>
</tr>
<tr>
<td>TRIA</td>
<td>Terrorism Risk Insurance Act 2002</td>
</tr>
<tr>
<td>TRIEA</td>
<td>Terrorism Risk Insurance Extension Act 2005</td>
</tr>
<tr>
<td>TRIPRA</td>
<td>Terrorism Risk Insurance Program Reauthorization Act 2007</td>
</tr>
<tr>
<td>TQM</td>
<td>Total Quality Management</td>
</tr>
<tr>
<td>VERIS</td>
<td>Vocabulary for Event Recording and Incident Sharing</td>
</tr>
</tbody>
</table>
Introduction

The cyber insurance market has existed in some form since the 1990s [1] but it is only since 2007 that the industry has started to see dramatic uptake in cyber insurance cover, albeit primarily in the US market. The global written premiums (GWP) for cyber insurance were estimated to total USD2 billion in 2015, a fraction of the total non-life insurance GWP of USD2,020 billion [2], but annual growth rates of cyber cover are around 25% and forecast to reach USD20 billion by 2025 [3].

Cyber risk is increasingly identified and accepted as a key business risk for all organisations, regardless of size. A number of high impact, high profile data breaches (the theft of Target retail stores’ 70 million customer database including 40 million credit cards in 2013, J.P. Morgan’s 76 million household accounts, health insurer Anthem’s 80 million record data breach in 2015 [4], and UK telecoms firm TalkTalk’s breach in 2015, to name a few) have brought to light the potential liabilities – legal, reputational, operational, financial – which all organisations face to varying degrees.

The average mean annual cost of cyber-crime for US firms is now USD7.7m according to a joint Ponemon Institute / HP report in 2015 [5]. The World Economic Forum’s 2016 Global Risks Report estimates that cyber-crime costs the global economy USD445 billion [6]. The report saw cyber risk enter its set of top 5 global risks in 2012 and 2014 and remain on its top 10 list of global risks in 2015 and 2016 [7]. The 2016 Allianz Risk Barometer survey placed cyber as a top 3 business risk overall (up from 5th place in 2015), and the top business risk in the UK, as well as being the main emerging risk over the long term for businesses [8]. In 2011 the UK Government rated cyber-attacks as a ‘Tier 1’ threat [9] (standing among threats such as international terrorism, military crises, major accidents or natural hazards) and in 2016 it announced a GBP1.9 billion pound investment in cyber security over the next 5 years [10].

Yet for the cyber insurance industry, cyber is an emerging risk. Although cyber risk is now firmly on companies’ risk registers (“88% of FTSE 350 companies now include cyber risk
within their strategic risk report, up from 58% in the previous year” [11]), the growth in insurance coverage outside the US has been slower. One of the aims of this study is to highlight the reasons for this and to outline the challenges facing insurers in spite of optimistic forecasted insurance growth rates of 150% over the next 5 years [12].

It is necessary to first examine the cyber risk landscape to identify the types of threats organisations face, as well as the recent trends and evolving risks which go hand-in-hand with the digitalisation of the workplace, and the interconnectedness of systems within and between organisations.

It is then useful to understand how businesses manage operational risk including the risk treatment process. This is followed by how cyber risk is defined and quantified for organisations and the types of cyber risk which organisations face.

Next, an overview of the insurance industry highlights the different professional risk carriers and lines of cover provided in the market followed by the insurability criteria of risk, specifically cyber risk.

To meet this risk, fully or in part, it is necessary to examine the types of cyber cover available, including the most common risks covered as well as the additional services provided by carriers to help manage risk ex-ante and ex-post a cyber incident. These services help insurers differentiate their offerings and provide additional benefit to insureds over and above financial indemnification for loss.

Chapters 6 and 7 cover the specific challenges facing both insurers and insureds. Of particular interest is the fast-changing legal and regulatory environments in Europe and the US. The current thinking is that the cyber insurance market is at a tipping point of major change [13], and the legal and regulatory environment will have a significant impact in its development.
Chapter 8 concludes with a future outlook of the insurance industry and the likely outcomes resulting from some of the specific challenges faced by insurers and insureds. In the face of uncertain risks and a lack of data, it seems certain that like the risk it covers, cyber products will continue to evolve and capacity will continue to grow. This may see a further specialisation of the market, or it may eventually be subsumed by traditional lines of insurance cover which have to date either excluded or limited cyber risks.

Interviews from various stakeholders in the UK and US insurance industry, UK Government, and wider investment community, are included where appropriate in the study, and the questionnaire and their full comments and transcripts are available in the Appendices.
1. The Cyber Risk Landscape

In developed and growing economies the use of information and communications technology (ICT) has grown over the past 30 years to encompass most aspects of everyday life. Individuals, businesses, and governments have all come to rely on interconnected digital devices which seemingly touch every industry and every walk of life. Technology has become so pervasive with the proliferation of different devices as well as their always-on and interconnected qualities. By 2020, the McKinsey Global Institute predicts [14] a market for between 20-30 billion connected devices and by 2025 the Internet of Things will have an impact of USD6.2 trillion on the global economy. Added to this is the observation [15] that we seem to prefer and rely on computing monocultures because the benefits of consistency outweigh any concentrated tail risks.

This combination of factors has brought incredible growth and productivity gains but we are now witnessing the growing rise of the accompanying risks of technology. Geer states ominously [15] that: “A technology that can give you everything you want is a technology that can take away everything that you have”.

1.1. Cyber Attacks

A cyber-attack has been defined [16] as: “deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks.”

Shackelford [17] categorises cyber-attack into 4 distinct types: cyber war, espionage (geopolitics), cyber-crime (financial gain), cyber terrorism (social causes such as Anonymous).

A 2016 report [18] by the Ponemon Institute into typical attacks faced by organisations found that among the main causes of data breaches, malicious or criminal attack accounted for 48% of all incidents, followed by system glitches (the result of IT and business process failures) at 27%, with 25% of all breaches caused by ‘human’ factors (defined as negligent
actions taken by employees and contractors). “InfoSec folklore” places a heavy emphasis on the insider threat but this doesn’t hold up to the facts as more than 80% of breaches in 2016 were carried out by external actors [19].

The barriers to entry to aspiring criminals have all but vanished in the digital domain. As demonstrated in Figure 1, the sophistication needed to carry out attacks has declined while the sophistication of tools to facilitate attacks has increased. The associated costs to carry out malicious activity have also decreased while the costs to prevent and defend against attacks have increased [20]. A recent report by the UK’s National Crime Agency highlights [21] how cyber-crime has now overtaken conventional crime.

Some commercial firms (such as the UK’s Gamma Group and Italy’s Hacking Team) and brokers or middlemen have made a business – also known as research-as-a-service [22] - from finding unknown exploits, also known as ‘zero day’ exploits, in widely-used software. Such exploits along with spam mailing databases can also to be found on a multitude of underground market websites.

_Crimeware-as-a-service_ encompasses a whole array of types of tools and services for would-be cyber criminals including malware (ransomware is an example of a current and growing threat) and exploits. _Crimeware infrastructure-as-a-service_ can be used to support a criminal operation, offering ‘bullet-proof hosting’ with which to launch denial-of-service attacks through the use of botnets or hosted spam services or illegal marketplaces (such as counterfeit pharmaceuticals). A fully outsourced service or _Hacking-as-a-service_ is also available for criminals with no technical expertise. Many underground services rely on feedback and reputation to engender trust which are familiar attributes of legitimate online marketplaces [23].

While tools and services have largely disintermediated the knowledge and expertise to conduct cyber-attacks, that is not to say that attackers are becoming less sophisticated. At the higher end of the scale, nation state funded activity whether conducting surveillance, espionage (including corporate espionage) and sabotage activities continues to grow.
Attacks on industrial control systems, included under the umbrella-term operational technology (OT), are also a growing concern. As the automation (and interconnectedness) of industry continues to grow, so do the associated risks. Cyber threats to OT have received increased attention in recent years particularly when the threats have been focused at critical national infrastructure [24]. The 2011 discovery of the highly advanced Stuxnet worm designed to enact physical damage to centrifuges used in Iranian nuclear facilities was a milestone in understanding the different possible scenarios in attacking industrial control systems.

More recently a blast furnace at a German steel mill was attacked and rendered unusable causing damages in the region of EUR240 million [25]. This attack was allegedly caused by accessing the plant equipment through the business IT infrastructure which is in itself an area of concern (where an attacker can pivot from an IT network into an OT network) [26]. In December 2015 the malware BlackEnergy facilitated an attack on the national power grid in Ukraine causing a power outage for around 225,000 customers. Much of the source code is now openly available leading to speculation that future attacks on industrial control systems may become more widespread [27]. In 2015 two security researchers managed to remotely control a vehicle’s dashboard computer via a software vulnerability prompting a recall of around 1.4 million Chrysler cars [28]. Medical devices have also been shown to be vulnerable to attack with a potential to cause injury or loss-of-life to patients relying on such devices, as well as opening a backdoor into a hospital’s IT systems resulting in a personal health record breach [29]. Some of these examples serve to demonstrate the potential or the realised physical damage, injury, and environmental damage which can happen as a consequence of industrial technology gone awry. These are also perils which would not typically be covered by traditional insurance lines of cover such as commercial general liability or property and casualty cover, and even rarely in standalone cyber cover.

With the forecasted growth of the Internet of Things (IoT set to become a pervasive presence in everyday life) [14], the challenge is to make security an enabling technology to engender the trust needed to rely on these devices; already one insurer has seen how it can
leverage IoT technology by partnering with a home security device manufacturer in order to offer innovative risk solutions, and more attractive premiums, to customers seeking home insurance [30]. This type of partnership may be the start of many within the insurance industry.

These examples of threats are just a handful from a continually evolving threat landscape. Some of the current trends are:

- The professionalisation or "commercialisation of cyber-crime" [33] which has driven up the frequency and severity of attacks. Crime-ware-as-a-service has brought increased sophistication, combined with ease of use, in tools and services used to conduct cyber-crime. The costs of offence (cyber-attack or cyber-crime) are constantly decreasing and the costs of defence are increasing. The challenge for government and industry is to close the gap [20].
- All organisations can expect to be breached at some stage: “No locale, industry or organization is bulletproof when it comes to the compromise of data” [19]. This is no longer the sole preserve of government organisations, large corporations or businesses in specific sectors such as healthcare providers or retail, pharmaceutical, defence, or financial services. For instance, information stolen from an SME or access gained inside an SME’s systems may facilitate a more lucrative crime particularly if the SME is a supplier to a larger firm (such as the 2014 Target breach). This has been described as a ‘secondary motive’ or something to ‘aid a different attack’ [19].
- Increasing reliance on interconnected (IoT) devices used by both consumers and business
- Industrial control systems which often rely on legacy hardware and software and which have been demonstrated to be vulnerable to attack. These attacks are particularly worrisome given their widespread use in critical national infrastructure
- Increasing sophistication of attacks on financial institutions through the use of malware such as Carbanak and others.
- Increasing sophistication of social engineering attacks such as spear phishing, business email compromise (BEC) scams, and ransomware.

These are just a few broad trends. The European Union Agency for Network and Information Security (ENISA) identified [34] fifteen specific threats to organisations in 2015, as shown in Table 1 below.

<table>
<thead>
<tr>
<th>1. Malware</th>
<th>9. Spam</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Web based attacks</td>
<td>10. Exploit kits</td>
</tr>
<tr>
<td>3. Web application attacks</td>
<td>11. Data breaches</td>
</tr>
<tr>
<td>4. Botnets</td>
<td>12. Identity theft</td>
</tr>
<tr>
<td>5. Denial of Service</td>
<td>13. Information leakage</td>
</tr>
<tr>
<td>7. Insider Threat</td>
<td>15. Cyber espionage</td>
</tr>
<tr>
<td>8. Phishing</td>
<td></td>
</tr>
</tbody>
</table>

Table 1 - ENISA Threat Landscape

Source: [34]
Of the risks identified in Table 1, ransomware is one threat worthy of further mention. ENISA described 2015 as the ‘year of ransomware’. New variants of ransomware quadrupled in the first half of 2015 alone and one variant, CryptoWall was estimated to have generated over USD300 million in revenues. Dr Andrew Coburn of Risk Management Solutions describes cyber extortion (or ransomware) as a “pernicious and growing [threat]” [35]. Beazley noted that the cases of ransomware it has dealt with had significantly increased from 2015 to 2016 [36].

Cyber threats will undoubtedly continue to proliferate, increase in sophistication, or evolve to exploit the weakest link in a system, which may be technical, physical, or human (for example, why try and break encryption when a legitimate user’s login credentials can be more easily stolen?). The challenge for companies is how these threats are tracked, identified, and quantified and then assessed and treated either through self-protection or self-insurance measures or through market insurance. The challenge for professional risk carriers is equally how to quantify the risks presented by cyber threats to price, productise, and commercialise risk transfer solutions to insureds and insurers.
2. Operational Risk

Operational risk has been described as “perhaps the most significant risk organisations face. Virtually every major loss that has taken place during the past 20 years, from Enron, WorldCom and Baring’s Bank to the unauthorized trading incident at Société Générale and the subprime credit crisis, has been driven by operational failure” [37].

Biener et al define operational risks as: “those arising due to the actions of people, systems and technology failures, failed internal processes, and external events” [38]. This definition is based on the Basel Committee on Banking Supervision’s own definition of operational risk as “the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events” [39]. The Solvency II directive which is aimed at harmonising insurance regulation and capital adequacy for insurers in the European Union takes an identical view [40].

Unlike market or credit risks where risk exposures are managed centrally, operational risk cannot be managed and treated centrally. As a result, robust operational risk management requires an appropriate governance structure and sponsorship of the executive management committee, accompanied by the right “tone from the top” [41].

2.1. Risk Management

“There is one and only one social responsibility of business — to use its resources and engage in activities designed to increase its profits” [42] wrote economist and Nobel Prize winner Milton Friedman in a New York Times article in 1970. Opinion on the supremacy of shareholder value has changed somewhat [43] in the intervening years but the idea of risk-taking and reward in the pursuit of profit go hand-in-hand. The National Institute of Standards and Technology (NIST) states that “understanding and addressing risk is a strategic capability and an enabler of missions and business functions across organizations” [44].
The corporate accounting failures of Enron and WorldCom and ensuing regulation (in the form of Sarbanes Oxley Act (SOX) 2002 in the US and the European Directive 2006/43, since amended by EU Directive 2013/34/EU and known as the Accounting Directive) prescribe the need to report on the adequacy of the organisation’s internal control on financial reporting [45]. An enterprise risk management framework such as that prescribed by the Committee of Sponsoring Organisations of the Treadway Commission (COSO), is widely used by US organisations [46] while ISO 31000 is largely used in other markets. A company’s Board sets the strategy and business model for the organization and the risk that goes with it, while management implements the strategy and objectives and associated operational risk management activities. Shareholders “have a responsibility to assess and monitor the effectiveness of Boards in overseeing risk... [but] are not themselves responsible for risk oversight at corporations” [47].

As part of an overall enterprise risk management (ERM) framework, an organisation will typically determine its risk appetite based on the culture of the organisation and its business strategy. It should also have a direct impact on the existing culture, helping shape a risk-aware organisational culture. The levels of risk – high or low – depend on the objectives of the business. In fact COSO explicitly states that organisations “must embrace risks in the pursuit of its goals” [48]. Rittenberg and Martens describe risk appetite as: “The amount of risk, on a broad level, an organization is willing to accept in pursuit of value. Each organization pursues various objectives to add value and should broadly understand the risk it is willing to undertake in doing so” [48].

The ISO/IEC 27000 family of standards is based on risk management principles and provides an information security framework which organisations can follow (and ultimately be independently assessed and certified if this is the organisation’s objective) to develop an information security management system (ISMS) to preserve the confidentiality, integrity and availability of information by applying a risk management process [49]. ISO/IEC 27005 provides a framework for implementing information security based on a risk management approach. Other commonly used frameworks include the Risk Management Framework, defined by NIST 800-37 and NIST 800-30, Risk IT, or COBIT published by ISACA, or internally
developed frameworks. Adopting a framework “establishes expectations for external relationships with organisations that will accept the transfer of risk, such as insurance carriers, as well as suppliers, clients, and business partners” [50].

Figure 2 provides an overview of how an organisation assesses and treats enterprise risk. The first step is to establish the context for the risk management process which defines the scope, organisation and boundaries for the process. Next, once the risk appetite has been developed, reviewed, and approved by management and the Board (and in alignment with business objectives), it must be effectively articulated and communicated within the organisation, monitored, and revised periodically as the needs of the business change (as part of a plan-do-check-act cycle). Policies, processes, and procedures can then be developed to help meet the business objectives (strategic, operations, reporting, and compliance in the COSO model) within stated risk tolerances. An alternative view would be to commence risk tolerance analyses and then look at the organisation’s risk appetite, the former being more straightforward than the latter [51]. Risk appetite has been described as a more qualitative measure whereas risk tolerance is more quantitative and these are the
basic building blocks from which a firm can begin to decide the proportion of risk retention and risk transfer activities that meet the firm’s risk profile.

A risk assessment of the business will look to identify and value the assets (from a baseline, quantitative or qualitative perspective, or combination of the two approaches, as defined in ISO/IEC TR13335-3) within the organisation such as the information assets, the infrastructure and systems, and people. According to [7] “Assessments must go beyond cybersecurity, as the risks are not just about external threats but also about the fundamentally unstable dynamics of digital infrastructures and the complex, chaotic and unpredictable ways they can interact with civic, social and economic systems”

A ‘crown jewel’ approach is commonly used given the pervasive and sometimes porous nature of organisational interconnected networks. That is, it may not be feasible nor cost-effective to protect every information asset, rather just focus on the critical assets which if stolen, damaged, or rendered unusable would severely impact business operations. The assessment process should then seek to identify any vulnerabilities to those assets concluding with a threat analysis identifying all types of threats and threat likelihood to those same assets.

Figure 3 demonstrates the risk treatment process. Risk Treatment is “the process of selecting and implementing of measures to modify risk”[52]. There are three stages to a risk treatment plan: the first is the input from the previous risk assessment stage, followed by the risk treatment action which requires a review of the risk treatment options, and finally the output which results in the plan itself, the satisfactory treatment of different risks identified and categorised in the action stage (the options being risk reduction, retention, avoidance, and transfer), and a list of residual risk i.e. not treated in the action stage.
In the second stage of the risk treatment process, as shown in Figure 3, there are four generally accepted types of risk treatment options resulting in a set of residual risks. [52] These options are:

1) **Risk avoidance**: any high likelihood, high impact risks which the business could neither treat nor wish to transfer and which could be terminated without materially affecting the business (risks 1-2 in Figures 4 and 5).

2) **Risk retention or acceptance**: this type and level of risk depending on the organisation’s risk appetite and risk tolerance may be acceptable and deemed the ‘cost of doing business.’ (risks 3-6 in Figures 4 and 5).

3) **Risk reduction or self-protection**: any risks the business can treat with people, process, technical measures (risks 7-8 in Figures 4 and 5).
4) **Risk transfer**: this is sometimes seen as tail end risk given its low likelihood but high impact. Typically, this kind of risk would be transferred out of the business to insurers, banks, and capital markets. It could also involve a hybrid solution where some risk is retained – such as a high risk business function – but the remaining risk may be outsourced to a cloud provider for payroll or HR services, an outsourced IT infrastructure company, a client support call or booking centre etc. These risks would be treated through service level agreements and contract (risks 9-11 in Figures 4 and 5).

A high level overview of these can be shown as a heat map in Figure 4 below. Each risk treatment option presents one or more possible courses of action for each risk presented. A single measure or combination of risk treatment options can be taken such as self-protection and risk transfer can be carried out for each risk as demonstrated in Figure 5.

![Risk Treatment Heat Map](source: Adapted from [53])
The residual risks that are left over from the risk treatment options are assessed as per the organisation’s risk appetite and may also need to be treated. The risk register keeps track of all identified risks, their owners, probability, impact, and treatment measures and should be reviewed on a periodic basis.

A common risk measurement metric used is risk-based capacity. One value is the difference between the enterprise value and book value of the firm and may be calculated as the amount of risk per share of stock. It could also be measured against other criteria such as EBITDA, a corporate debt rating downgrade or by violating a banking covenant [51]. These are hard metrics and relatively straightforward to measure. Risk appetite may be more of a ‘gut feel’ about what the organisation should or should not be doing and would likely align with the business activities and culture of the firm.

Another metric which affects the decision on risk retention levels is the total cost of risk of the organisation. This may be calculated as the total self-insured losses and expenses which form part of the firm’s risk management along with any third-party insurance premiums. A critical factor in this calculation necessitates an evaluation of the cost of capital [54]. If the cost of capital to retain and treat the risk is less than its transfer via insurance, then this
would naturally favour more risk retention. It may therefore be better to turn to the banks for a loan or the capital markets with a debt issuance to self-insure and self-protect.

In determining risk treatment Bolot and Lelarge demonstrate [55] that most cyber security activity today is concentrated on risk retention and self-protection and that most research to date has focused on self-protection. Furthermore, “self-protecting against risk or mitigating risk does not eliminate risk”. So the question then becomes, “how to handle the residual risk”? This can be done through contract or hedging but is commonly achieved by taking some form of insurance cover. This could involve both self-protection or self-insurance as well as third-party or market insurance and will be examined in more detail in chapter 3.

Therefore, as part of an overall enterprise risk management process an organisation seeking to transfer any residual risk will typically insure against low frequency high impact risks by purchasing insurance policy. This cover is for a defined peril (or set of perils) in a given timeframe for a set of assets made by entering into contract with an insurer and paying a premium with a defined limit of cover. The insuring entity could be one specifically set up to serve the organisation or like-minded organisations (such as within a particular industry) known as a captive or one which offers lines of cover to all organisations. We will look in chapter 5 at the types of cover currently available in the market.

Insurers seeking to treat their own enterprise risks would follow a similar process of self-protection measures to sharing commercial risk by forming syndicates of insurers or through reinsurance (or other mechanisms such as establishing side car vehicles and issuing insurance linked securities such as catastrophe, or, cat bonds). The different ways insurers and reinsurers treat their own risks will be examined in greater detail in chapter 6.

It is also worth noting that different stakeholders of organisations have different viewpoints on enterprise risk. Shareholders of public companies (which may also include (re)insurers) look for a return on capital invested in the company and are primarily interested from a performance measurement perspective. Policy holders of insurers and industry regulators
(such as the Prudential Regulation Authority in the UK) are concerned with the insurers’ ability to pay claims and not breach capital solvency requirements (or ultimately become insolvent). Managers of companies will seek to balance the needs of shareholders as well as policy holders and regulators and thus require a more detailed risk assessment of the organisation understanding risk loadings in pricing, business performance, and capital allocation [56].

2.2. Cyber Risk

The Allianz Risk Barometer describes cyber risk as the most underestimated risk facing businesses and that there is no one ‘silver bullet’ solution to cyber security [33]. From an insurance perspective cyber risk (and cyber cover) is still seen as an emerging risk. The World Economic Forum identified cyber risk as one of the top global risks since 2012 and characterises cyber risk as: “Misbehaviour by employees, industrial espionage, and cyber-attack are among the greatest dangers that companies face in the big data era” [57]. More specifically, Airmic, the UK insurance and risk management association recently defined its 3 main areas of cyber risk as: business interruption, loss or theft of data, and reputational damage [58].

At a general level, cyber risk is “synonymous with IT risk” [11], and given the extent to which organizations today rely on technology for internal control purposes, enterprise risk management frameworks such as COSO or ISO 31000 [59] will typically place cyber risk within the sphere of operational risk. As such, operational cyber risk can be defined as “operational risks to information and technology assets that have consequences affecting the confidentiality, availability, and integrity of information and information systems.” But its enterprise-wide reach will also intersect with business, strategic and financial risks along with compliance and reputational risks. External risks such as market, and credit risks may also be impacted in the event of a cyber-related incident.

It can also be argued that some ERM frameworks, particularly one such as COSO which is still in practice focused on internal control, are inappropriate for measuring a dynamic risk
such as cyber risk. “A complex approach (as often is the case in control/compliance-based approaches) on top of a complex and changing dynamic environment, tends to increase risk – the opposite of the desired objective” [60]. Other methods such as Root Cause Analysis (RCA) may be better adapted for cyber risks.

Biener et al [61] and Cebula and Young [38] categorise operational cyber risk based on the Basel Committee definition of operational risk which can be broken down into 4 areas:

1. **Actions of people** – actions can be malicious or with intent, or through negligence by performing a negligent act or through inaction
2. **Systems and technology failures** – these cover hardware, software and systems failures
3. **Failed internal processes** – process design or execution, process controls, supporting processes
4. **External events** – catastrophes (man-made or natural), legal and compliance issues, business and market conditions, dependencies on third parties

Each of these categories is outlined in more detail in the Appendix III.

A critical insight in creating this taxonomy was that risks can have a knock-on effect such that “risks can cascade: risks in one class can create risks in another.” The World Economic Forum’s 2013 Global Risk report coins the use of social media as a kind of ‘digital wildfire’ but this could easily equate to cyber risk at a more general level [62]. In the underwriting world this is key to understanding aggregation risk in any particular line or lines of cover.

As an operational risk, cyber risk affects insurers – as organisations – as much as their clients, the insureds. In some ways the risks can be greater as insurers are prime targets for attackers interested in stealing their valuable data sets. Personally identifiable information (PII), and particularly personal health information (PHI), can fetch much higher values per record than credit card information [63] [18].
As professional risk transfer carriers, insurers also take on the transfer of risk from their clients which in itself involves additional risk management processes. The Chief Risk Officers Forum identified the following challenges for insurers in assessing cyber risk [64]:

1. **Insufficient or poor quality loss information** – there is limited loss data (i.e. low numbers of claims), and the available historical loss data does not necessarily reflect the current environment given the fast-moving threat landscape.

2. **Uncertain value of loss information** – unlike other well-established lines of cover such as property and casualty there is no established calculation method to quantify cyber risk and again, unlike other lines of cover, there is either no information or limited information sharing (the reasons for this are explained in further detail in chapter 6.3). The intangible nature of cyber-attacks also only further complicates its quantification: an attack may not become apparent until months after an initial breach, nor will the provenance of the attack be necessarily determined. An attack on one system may also be part of a wider attack on several systems or a pivot into another system such as a third-party supplier to a larger firm.

3. **Highly interconnected IT systems** – not only are IT systems interconnected but the hardware and software used to run the systems are produced by a relatively small number of companies. Software has become highly complex, often developed using common code libraries (some open source) sometimes leading to vulnerabilities (e.g. the OpenSSL Heartbleed [65] and Symantec products vulnerabilities [66]) while maintaining legacy code which can also be a source of vulnerability. As a result, the concentration of risk centres around a number of widely used systems which are themselves highly interconnected. This presents aggregation or accumulation risk and is why cyber risk is often described as a systemic risk. A cyber catastrophe can be defined as a: “systemic event that impact many organisations at the same time, causing many of them to suffer significant losses” [67].

4. **Continually evolving attack strategies, perpetrators and motives** – cyber risk has been described [68] as a not unfamiliar risk for the industry albeit with a different look and feel, and it is a risk which is emerging in different ways. It is this dynamic
nature of cyber risk which involves both technological and human factors and which has led to a perpetual arms-race to keep up with new and evolving threats.

These are all key risks for insurers and the challenges for insurers will be explored in more detail in chapter 6.
3. Overview of Insurance

Insurance has been described as “a crucial part of the DNA of capitalism, allowing people and companies to take the risks they need to take” [69].

The concept of insurance has existed throughout the ages in the shape of guilds and benevolent associations but the modern form of insurance we know today was born towards the end of the 17th Century. Edward Lloyd’s coffee house on Tower Street in London opened in 1688 and like other coffee houses in the city developed a specialist interest where merchants and entrepreneurs would meet [70]. Lloyd’s specialised as a venue providing shipping news, later developing into a market place to insure ships and cargo. As London’s importance as a trade hub grew, the demand for marine insurance grew with it. The second major impetus to the insurance market grew after the great fire of London in 1666 providing the origins of property insurance. Today, Lloyd’s is the ‘oldest, continuously active insurance market place in the world’ [71] and the UK is the third largest market in terms of premium income after the US and Japan, although soon to be eclipsed by China [72].

![Figure 6 - The Insurance Chain](image-url)
Insurance can be defined as: “A contractual relationship that exists when one party (the insurer) for a consideration (the premium) agrees to reimburse another party (the insured) for loss to a specified subject (the risk) caused by designated contingencies (hazards or perils)” [73]. Majuca et al highlight [74] two different perspectives on insurance: from the insurer and the insured: “(1) the insurer who seeks to capture profit from premiums exceeding losses over time by spreading the risk of uncertain loss events across many independent clients, and (2) the individual or organization who seeks to maximize their utility/profit by managing the risk of uncertain loss events.” Later in this study we will examine the perspectives from both of these entities.

The insurance industry is broadly divided into life or non-life lines of cover (also known as general insurance). General insurance is further divided into primary lines and excess lines. Of the types of commercial insurance offerings available, the most common lines are Property & Casualty, Commercial General Liability, Professional Indemnity (also known as Errors and Omissions (E&O) in the US market), and Directors and Officers (D&O) insurance.

Risk transfer as a commercial activity is shown in Figure 6, and provides a simplified overview of the ‘Insurance Chain’. A commercial organisation would typically seek third party insurance from a professional risk carrier. This could be sought via an intermediary (a broker), direct to an insurer, or direct to a reinsurer. The organisation could also combine this third party insurance with a self-insurance mechanism such as a captive organisation. This could be used for tax purposes but also because of a lack of market capacity or high costs to cover particular risks. A captive is commonly funded and owned solely by its parent company (i.e. the commercial organisation) [75] and known as a pure sole captive (or single parent captive); equally, the captive can have multiple owners (sometimes in the same industry) and is known as a pure group captive. Sponsored captives are managed by unrelated entities and do not necessarily pool risks with other members. [76] Captives, like insurers may transfer some risks to reinsurers, and reinsurers can in turn transfer risks to retrocessionaires (other reinsurers). All three entities may tap the capital markets to transfer risk and/or raise capital using insurance linked securities (ILS). Institutional
investors (including pension funds, insurers, asset managers, sovereign wealth funds, hedge funds) hungry for alternative and uncorrelated asset classes with attractive yields and low volatility, invest in different types of ILS. In fact, the ILS market is set to double in size by 2019 to USD 87 billion [77]. ILS are explored further in chapter 6.7.

3.1. Insurability Criteria

One of the fundamental tenets of insurance is the process of determining whether or not risks are insurable. A set of criteria was devised by Berliner in 1982 specifically to look at the insurability of risks from an insurer’s perspective [78] [79]. These criteria were grouped into three broad areas: actuarial, market, and societal, as interpreted by Biener et al [61] and listed in Table 2.

<table>
<thead>
<tr>
<th>Type</th>
<th>Insurability criteria</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actuarial</td>
<td>Randomness of loss occurrence</td>
<td>Independence and predictability of loss exposures</td>
</tr>
<tr>
<td>Actuarial</td>
<td>Maximum possible loss / probable maximum loss (PML)</td>
<td>Manageable</td>
</tr>
<tr>
<td>Actuarial</td>
<td>Average loss amount per occurrence</td>
<td>Moderate</td>
</tr>
<tr>
<td>Actuarial</td>
<td>Average period of time between two loss occurrences</td>
<td>Loss exposure must be large</td>
</tr>
<tr>
<td>Actuarial</td>
<td>Information asymmetry</td>
<td>Moral hazard and adverse selection must not be excessive</td>
</tr>
<tr>
<td>Market</td>
<td>Insurance premium</td>
<td>Cost recovery and affordable</td>
</tr>
<tr>
<td>Market</td>
<td>Insurance cover limits</td>
<td>Acceptable</td>
</tr>
<tr>
<td>Societal</td>
<td>Public policy</td>
<td>Consistent with societal value</td>
</tr>
<tr>
<td>Societal</td>
<td>Legal restrictions</td>
<td>Allow the coverage</td>
</tr>
</tbody>
</table>

Table 2 - Berliner Insurability Criteria

Source: [61]

Bruggeman [80] adds to the Berliner criteria by including an actuarial condition that the risk must be measurable in terms of its likelihood; secondly, a market condition must be that there is sufficient industry capacity to cover the risk.
A further exploration of the nine insurability criteria will be performed looking at the applicability of cyber risk in chapter 4. What is important to note is that a risk can be uninsurable for the professional risk carrier if any one of these criteria is not met. [79]
4. Cyber Insurance

4.1. Growth of Cyber Insurance

The first cyber policies were devised in the 1990s [81] and were essentially ‘hacker’ policies to cover third-party liability for the effects of malware. From 2003 when the first US data breach laws came into existence in California, cyber cover grew out of necessity to comply with US State (and federal) regulations on the unauthorised disclosure of personal information.

By 2008 as one survey put it “cyber insurance is a concept that has a great deal of intellectual appeal, has seen a degree of implementation, but that isn’t taking the enterprise world by storm.”

Since then, however, demand for insurance continued to grow, and the US now holds the lion’s share of the cyber insurance market at approximately 90% of the USD 2 billion global market. The market as a whole is, by one estimate, predicted to grow up to USD20 billion by 2025 [3] [33]. However, the geographic balance could be reset in the coming decade as European data privacy regulation, which carries stiff penalties for non-compliance, is set to take effect from 2018.

A 2015 survey saw cyber risk appearing ‘dramatically’ for the first time in its risk leader board [82] ranking number 4 out of the top 10 risks. Survey respondents indicated that the growth in cloud computing and the amounts and types of data held in the cloud, raised financial and reputational concerns caused by ‘inevitable’ breaches. In non-life insurance, cyber was the number one identified risk in Property and Casualty indicating the growing underwriting risk for cyber.
4.2. Cyber Insurability Criteria

Using the Berliner insurability criteria outlined in chapter 3, the insurance requirements are examined from a cyber risk perspective in more detail below. Figure 7 graphically represents some cyber risk characteristics within these criteria from the perspective of how problematic each one is to satisfy.

1. Randomness of loss occurrence

The quantifiable risk is unexpected and unintended and the correlation to other risks is minimal.

One of the characteristics of widely used IT and OT systems is their monoculture in operating systems and principal applications (such as Microsoft Windows and Microsoft Office in a desktop environment, Android and iOS in mobile devices, Cisco in routing and switching infrastructure, Siemens in Supervisory Control and Data Acquisition – SCADA – systems, operational technology used in manufacturing). Another characteristic is the connected nature of information technology systems and devices which all connect to the internet. Both characteristics combined present a serious concentration and correlation of risk, should any IT system be compromised. The Mydoom malware which first struck in 2004 caused an estimated USD38 billion in damages making it one of the most damaging exploits of the decade [83]. However, some evidence also exists showing that most cyber risk incidents are not correlated, or that correlation does not exist in all categories of cyber risk [61]. The quantification of cyber risk is one of the most problematic areas for insurers. The pool of underwritten risks should be as uncorrelated as possible so that one loss event does not cascade and trigger other underwritten risks within the same pool.

2. Maximum possible loss

The total potential loss from an insured peril is manageable.

Based on analysis [61], cyber risk losses to date are still well below non-cyber (other operational) risk losses. Insurers protect themselves through cover limits, policy wordings, deductibles, and through the setting of appropriate premium levels. The insurers’ risk is also off-set through risk-sharing via syndicates or reinsurance.
A recent UK Government / Marsh report estimates that the likely probable maximum loss (PML) of insured losses from a global cyber event is in the region of GBP20 billion from a total loss of USD100 billion [11]. Another report [24] put the potential PML of up to USD71.1 billion resulting in a cyber-attack on the US power grid out of economic losses of between USD243 billion and USD1 trillion. This is one of the reasons cyber is often equated to natural catastrophe risk in terms of high potential loss amounts. But the risk of large-scale cyber-attacks and evidence of the growing frequency of attacks, combined with the growing hyper-connectivity of internet-connected devices (i.e. IoT devices), only serves to heighten the aggregation risks of cyber [7].

3. Average loss amount per occurrence

*The average loss from an insured peril should be manageable.*

Insurers protect themselves through cover limits and policy wordings. According to IBM and the Ponemon Institute [18] the average loss from a data breach was almost USD4 million in 2015, a 29% increase since 2013.

4. Loss exposure

*There should be a sufficiently high number of independently exposed loss events to enable the calculation of expected losses for the insured risk.*

In other words, the accuracy in calculating expected losses increases with an increased amount of data. This is a principle known as the law of large numbers and underpins the economics of insurance [61].

5. Information asymmetry

*Moral hazard and adverse selection must not be excessive.*

Information asymmetry is common between buyers and sellers and happens when one party has an information advantage over the other party. An insurer will in practice have less information about the buyer/the insured which presents certain risks to the insurer. Adverse selection characterises this risk, and may result in the insured not disclosing all relevant information which the insurer needs to accurately price a differentiated premium.
and cover given, based on the risk profile of the insured. As such, insurers may in theory offer low-premium low-cover policies for low risk insureds and high-cover high-premium to target high risk firms. This leads to inefficient markets or ‘lost dissipative social welfare’ [74]. Insurers protect themselves against information asymmetry through policy exclusions, retention levels, deductions and policy limits but also through an in-depth ex-ante initial application process. This may involve not only a detailed questionnaire to understand the size, business, and risk profile of the insured, but also a mapping out of the security measures of the insured and even intensive investigation such as pen-testing or on-site assessments. This allows insurers to differentiate between low and high risk clients and set policies accordingly.

Against the backdrop of information asymmetry, moral hazard is the principle by which insureds are incentivised to modify their behaviour to ‘keep them honest’. By adopting certain ongoing security measures or risk management activities (such as using online risk management tools and training resources [84]), the insurance premiums may be reduced. This investment in self-protection, as a requirement of insurance, is important in demonstrating how cyber insurance may have a positive impact on an insured’s overall security posture. Policy wording and exclusions also have an effect on moral hazard. This will likely require the insured to maintain the same level of security throughout the policy term at the time of the ex-ante assessment, or risk not being covered in the event of a breach. This is why it is important for policies to be clear about the cover offered, to reduce the risk of legal recourse in the event of a disputed claim.

One alternative incentive for addressing moral hazard was highlighted recently in a government report [85] evaluating the aftermath of the 2015 data breach of UK firm TalkTalk. One of the findings suggested that to “ensure [cyber] receives sufficient CEO attention before a crisis strikes, a portion of CEO compensation should be linked to effective cyber security.” In an era of increased scrutiny of executive pay by media, government and institutional shareholders, this proposal may gain wider support. If that happens, cyber risk will become a business imperative for all UK-listed firms.
Information asymmetry will always be a challenge for insurers in offering and pricing cyber cover in that the security measures firms use to protect their assets use a combination of “technical and human factors and their interaction, [and] surveys can’t perfectly quantify risk”[86].

6. Insurance premium

*Cost effective for the insurer and attractive to the insured.*

The insurance premium should be set at a level which is attractive and affordable to the insured but adequate to cover the insurer’s expected claims for the line of cover minus costs and solvency requirements.

Although the overall insurance market is going through a soft cycle with plenty of capacity and competition [84] there are indications [12] that the cyber market is hardening particularly in certain sectors such as retail and healthcare. Insurance premiums for cyber are set at higher prices than other lines of liability coverage given the lack of certainty in quantifying cyber risks and due to losses from claims made. Currently, this is approximately three times the cost of cover compared to other general liability cover [11]. It is also likely that premiums will continue to rise from 10%-200% [12].

7. Insurance cover limits

*Insurance needs to be acceptable for the risks covered.*

The line or lines of cover defined in the insurance policy will have conditions which trigger the claims process (such as occurrence of the peril or on a ‘claims made’ basis) and set financial limits of the line of cover. Policies in both traditional lines and standalone cyber cover will contain exclusions of certain perils which trigger cover. Insureds may also be required to retain a quantum of risk – a retention level – before policies pay out. Although policy limits are increasing, they are arguably still not high enough. [25] There should also be sufficient capacity in the industry to cover the underwritten risk. This area is particularly problematic for both insurers and insureds.
8. Public policy

*Insurance should be consistent with societal values.*

Insurance should provide cover for relevant risks and not incentivise criminal activity. This raises the issue of moral hazard where it is possible that insureds may be less incentivised to carry out self-protection activities, and therefore raise the overall risk exposure for the industry.

9. Legal restrictions

*A jurisdiction should allow the insurance cover.*

Insurance needs to function within a reliable legal framework and should only provide cover for permitted risks. Cyber risk is an evolving risk and therefore challenging to cover to comply with varying jurisdictional requirements. One potential area of concern for insureds is that some jurisdictions do not allow insureds to receive indemnity for regulatory fines.

As outlined above and highlighted overleaf in Figure 7, the main problematic areas within the insurability criteria are (1) randomness of loss occurrence, (5) information asymmetry, and (7) limits of cover. All three criteria are problematic to insurers but limits of cover equally affect insureds given the dynamic risk nature of cyber, the consequent difficulty in quantifying and pricing it, and the non-standardised and potentially confusing offerings in the market.
Figure 7 - Assessment of Cyber Risk

Source: Adapted from [61]
5. Types of Cyber Cover

Although the first cyber cover goes back to the 1970s [87], the first ‘hacking’ insurance policies became available in 1998 when technology companies partnered with certain insurers to offer technology solutions combined with liability cover from a loss event [74]. The likes of AIG, Hiscox, and CFC Underwriting were among the first to provide this type of insurance cover. Gradually, policies evolved to cover damage to the insured’s own property so that today most policies, like many other categories of cover, offer a combination of both first- and third-party cover.

However, the majority of market demand for cyber insurance products has until present mainly been driven to comply with US privacy regulation and these products are designed to indemnify, and in some cases provide additional services, as a result of a data breach. The question now is whether businesses will start to take a more holistic view of cyber risk, and if so, whether this will spur the ‘next wave’ of cyber insurance [88]. Or, will the next wave of demand be again driven by data privacy regulation in the form of the 2018 EU GDPR?

The types of cover split between first and third-party cover can be summarised in Table 3. Excluded cover typically centres on property damage and casualty, including bodily injury, death, and terrorism.

<table>
<thead>
<tr>
<th>First party</th>
<th>Third party</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical damage: people and physical assets</td>
<td>Privacy, confidentiality, and security liability</td>
</tr>
<tr>
<td>Damage to digital assets (software and data)</td>
<td>Multi-media liability</td>
</tr>
<tr>
<td>Business interruption</td>
<td>Cyber-attack on a third-party from breach of</td>
</tr>
<tr>
<td></td>
<td>insured systems</td>
</tr>
<tr>
<td>Cyber Extortion, ransomware</td>
<td>Content injury</td>
</tr>
<tr>
<td>Customer care and notification expenses</td>
<td>Loss of third-party data</td>
</tr>
<tr>
<td>Reputational loss</td>
<td>Outsourcing - damages and defence costs</td>
</tr>
<tr>
<td>Theft: Intellectual property, commercially</td>
<td></td>
</tr>
<tr>
<td>sensitive data, financial</td>
<td></td>
</tr>
<tr>
<td>Cyber-attack from a breach of a third-party</td>
<td></td>
</tr>
<tr>
<td>system</td>
<td></td>
</tr>
<tr>
<td>Regulation defence and fines</td>
<td></td>
</tr>
<tr>
<td>Bodily injury and death</td>
<td></td>
</tr>
</tbody>
</table>

Table 3 - Categories of First and Third-Party Cover
A more exhaustive look at actual examples of cover in the market are consolidated in Figure 8 overleaf which compares results from Marsh, the University of Cambridge’s Centre for Risk Studies (CCRS) and Risk Management Solutions (RMS). The cells highlighted in blue are the main areas of cover identified by both firms and where they are positioned within the RMS schema. To the left of Figure 8 are the top ten areas of cover identified by RMS and their percentage of occurrence in the 26 different policies it examined. Data and software loss and incident response costs are grouped together at 81% due to the same number of occurrences in policies. Data privacy breach, unsurprisingly, is the most common type of cover provided, followed by loss of data and software, cyber extortion, and business interruption. Reputational damage cover is provided by half of policies. At the bottom of the table are categories of cover such as intellectual property (IP theft), physical asset damage and death and bodily injury.
Outside standalone lines of cyber loss cover there may also be limited or full cover included within traditional lines (P&C, CGL) of cover, explicitly or implicitly endorsed (also known as silent cover). The latter is something which Lloyd’s has asked its members to fully understand and quantify the potential exposure in case of claims, and is further examined in chapter 6.4.

**Figure 8 - The Top 10 Most Common Categories of Cyber Loss Cover Across 26 Different Categories**

Source: [89]
5.1. Add-On Services

The cyber insurance market developed as a handful of partnerships between technology firms and underwriters. That dynamic has grown and many (re)insurers also look to grow in-house expertise for emerging and fast growing OT risks [90]. That may also include partnering with specialist firms to provide particular elements of a breach response service (e.g. pen testing, forensics, or legal advice) [91]. Both in-house expertise and partnerships serve insurers in a couple of ways: firstly, cyber risk expertise can assist in the underwriting process, and secondly, offering a suite of services (or a ‘turnkey’ product) can be a strong incentive to purchase cover. There are 2 main areas where additional services can assist insureds: before, ex-ante, and after, ex-post, an incident.

5.1.1. Ex-Ante Services

*Ex-ante* services are generally classed as risk management services. The types of services provided range from risk assessment and scoring tools provided by firms such as BitSight Technologies, Pivot Point Risk Analytics, and SecurityScorecard [92]. Other services could offer online training on common or emerging security threats.

The benefits to the insured may be to encourage self-protection activities but also to gain more favourable premiums. Although it is usually better to avoid a loss where possible rather than making a claim on insurance [93].

5.1.2. Ex-Post Services

*Ex-post* services typically cover the largest expenses for insureds. In fact, partnerships with specialist security firms come at a high cost: one area of concern for insurers is the rising cost of breach response [93]. This has been higher than expected and may contribute to carriers increasing premium rates.
Beazley Breach Response (BBR) Services dealt with 955 data breaches so far in 2016 on behalf of clients, compared to 611 breaches in the same period in 2015 [36]. The benefits to relying on the insurer are in the coordination of different types of expertise: forensics, legal, PR, notification, and credit monitoring. Limits and restrictions may be put on each of these services. For example, an insurer may place certain conditions on the use of such services and will indeed place aggregate limits on their costs. It may provide a preferred list of legal firms rather than allow the insured to retain their own counsel. But the grouping and inclusion of such services within the policy is an attractive proposition to the insured.

The incentives are clear for insureds to carry out self-protection activities such as a deployment of technology (e.g. encryption, perimeter controls, or data loss prevention tools) in order to bring down premiums. This investment in appropriate levels of self-protection, along with the insurers’ breach response services (as well as financial indemnity and legal liability cover), may well be a compelling proposition and one which could raise overall levels of security.
6. Challenges Facing Insurers

The cyber insurance market presents new opportunities for insurers in what is currently a soft market, with excess capacity and marginal or negative growth in many existing risk categories [94]. Aon Benfield reports [88] a bifurcation growing in the insurance market between existing and emerging risks and argues that the latter, which includes cyber risk, will be the ‘growth engine’ for the industry over the next decade. With an annual growth-rate of 150% and an estimated USD2 billion in premiums [3], and forecasts of between USD7.5 billion and USD20 billion by 2025, cyber insurance is growing at an impressive clip [33]. In contrast, the overall cyber security market (i.e. the self-protection market) is estimated to grow from USD 122.45 billion in 2016 to USD 202.36 billion by 2021 [95].

As such, cyber could become a major line of business for insurers within the next 10 years [88]. Equally, the market could just ‘fizzle out’ as cyber exclusions in traditional lines of cover are reduced or removed, paving the way for a ‘cyber’ element of cover in all insurance policies [25] [68].

This growth brings opportunities for the industry but also raises a number of key risks for insurers. These include a lack of historical claims data, gaps in insurance cover which insurers may be implicitly liable for if claims are triggered, risk accumulation both at an insurance and reinsurance level, adverse selection and moral hazard, and a constantly evolving threat landscape.

6.1. Legislative Drivers

‘Hacking insurance’ kick-started the industry at the end of the 1990s but it was only once US data privacy legislation came into force in the early 2000s that the cyber insurance industry gained significant traction [84].

California initiated the first of the US State breach notification laws in 2003 aimed at organisations owning or processing personal information and suffering an unauthorised
breach; since then, 46 other states have followed suit (with the exception of Alabama, New Mexico, and South Dakota). California distinguishes between different types of personal information (medical, personal, health, business records) and similarly each state may also have different definitions as to what constitutes personal data [96]. There have been efforts to pass a federal law which would pre-empt state laws as each state law has its own different requirements and definition of personal information and breach notification rules. This imposes huge costs on the need to ensure compliance with every state where an insurer or business operates and processes personal information. The estimated notification costs, as a result of the data breach at US health insurer Anthem in 2015, could total USD40 million alone [97].

However, two federal laws in particular are key to businesses and insurers holding personal information and which have driven the demand for insurance: the Gramm Leach Bliley Act (GLBA) passed in 1999, and the Health Insurance Portability and Accountability Act (HIPAA) passed in 1996, cover specific industry security requirements for protecting personal information in the financial services and healthcare industries, respectively [98]. The Health Information Technology for Economic and Clinical Health (HITECH) Act which passed in 2009 was brought in to strengthen HIPAA by imposing financial penalties through the Office of Civil Rights (OCR) [99]. Sarbanes-Oxley Act (SOX), the Payment Card Industry Data Security Standard (PCI DSS), and the Federal Information Security Modernization Act of 2014 (FISMA) were also important standards or laws in driving reporting, internal control and security requirements, as well as demand for cover. Other federal laws such as the Privacy Act 1974, The Freedom of Information Act (FOIA), and the Family Educational Rights and Privacy Act (FERPA), outline rights for protecting personal information. Today, the majority of cover in the US is driven by the need to comply with such regulation and to cover the costs in the event of a data breach.

Insurers themselves are prime targets for criminals. In 2015, the U.S. National Association of Insurance Commissioners issued a guidance document [100] laying out ‘12 principles for effective security’ in the wake of high profile data breaches in 2014/15 at US health insurers CareFirst BlueCross BlueShield, Premera Blue Cross, and Anthem (the largest breach at
almost 80 million records). The onus is on the state insurance regulators to promote the adoption of effective and uniform security standards in the insurance sector for data and infrastructure to protect consumers’ data.

EU member states have also had their own data privacy laws for some time, some of which consolidated existing laws to meet the requirements laid down by the EU Data Protection Directive in 1995 [101]. Like the US in the last decade, Europe may see similar demand for cover with the impending General Data Protection Regulation (GDPR) taking effect from May 25th 2018. The regulation which will be immediately effective [102] in all EU member states aims to harmonise and strengthen data protection rules for individuals and will apply to all firms (including foreign companies) which process or control the personal data of EU residents. Penalties for data controllers or processors infringing the regulation are high with potential fines totalling up to EU20 million or 4% of the firm’s global turnover (whichever is greater). The implications for UK based firms controlling or processing data following the 2016 ‘Brexit’ referendum are likely to be equally applicable and therefore will apply to UK insurers with exposure to EU personal data as well as their insureds which may have business activities involving the use of such data. Although the UK has already had a Data Protection Act since 1998 [103], the fines levied by the Information Commissioner’s Office are capped at GBP500,000 [104], although insurers are liable for much higher fines imposed by the Financial Conduct Authority (insurers in the UK have received fines of GBP2.25 million and GBP3 million for data breaches) [105]. The GDPR fines could have a massive financial and reputational impact on businesses which become victim to breaches. For insurers, some uncertainty lies around the insurability of fines, unlike in the US, as there is a “lack of case law and procedure” [106]. Although it is unclear how GDPR will work in practice, the onset of regulation is likely to drive demand for cover [68].

As data breaches continue to proliferate in high risk industries such as health care, retail, and education, and new threats evolve – such as ransomware (or reappear, as the first known case of ransomware was the Aids Info Disk Trojan in the 1980s [107]) – new business risks appear, or existing covered risks such as business continuity are now impacted by cyber. Aon Benfield predicts [88] that businesses will drive the next wave of cyber insurance
as they start to take a more holistic view of cyber risk and the wider impact it may have on business operations. Already, Beazley sees the US market shifting as insureds are starting to broaden their requirements from data breach cover to business interruption cover [108]. This may be a sign of a maturing market [90] or this may reflect the growing threat from ransomware and its consequent impact on business continuity. Beazley had 43 ransomware incidents in 2015 yet the first half of 2016 had already doubled the incidents [108]. For healthcare companies which store and process PHI, these incidents may not only fall under HIPAA breach reporting requirements for PHI (there is still some legal ambiguity around this depending on how the ransomware affects the data and whether unsecured PHI is disclosed [109]), but more critically, a ransomware incident affects the day-to-day operations of the organisation and could have a material impact on revenues and reputation. Of additional concern is that the full picture of ransomware incidents is not known because businesses are generally reluctant to disclose such incidents voluntarily [110].

In Europe, Beazley has mainly seen demand for business interruption cover compared to other lines of cyber cover. This may change once the GDPR becomes effective as insureds look to include data breach cover to minimise this new regulatory risk. According to Allianz [33] although liability and data protection will continue to be areas of concern, business interruption risk will emerge as a key risk within the next 10 years.

Another area of change in the European market, and one which may drive the up-take of cyber insurance, is the Network and Information Security (NIS) Directive which came into effect in the EU from 1st June 2016. The Directive applies to operators of essential services (in sectors determined by the Commission but largely in areas touching critical national infrastructure) and digital services providers (cloud providers, search engines, online market places). Certain technical and organisational measures will have to be undertaken to varying degrees by both groups along with different incident reporting obligations [111]. Both the GDPR and the NIS Directive should help build a better aggregate picture of threat and breach data under their mandatory disclosure requirements.
6.2. Lack of Data

A key challenge in quantifying cyber risk is a lack of data. This impacts every aspect of cover including the [correct] pricing of premiums, limits of cover, exclusions, along with how an insurer itself transfers in part (or in whole) the underlying risk with other professional risk transfer carriers (such as reinsurers).

The Association of British Insurers’ (ABI) head of strategy breaks this down [102] into a couple of areas: firstly, *real-time threat intelligence* gained from a ‘handful’ of sources through the Cyber-security Information Sharing Partnership scheme (CiSP) which is part of the UK Computer Emergency Response Team (CERT-UK). The main challenges are that any information that is shared with CiSP is done so on a voluntary basis. Although CiSP has 2225 member organisations, it is primarily driven by large businesses in a small concentration of industries. Organisations, unless required by law, are reluctant to share breach data due to the likely reputational damage and loss of confidence from different stakeholders (clients, partners, suppliers, shareholders); secondly, *pricing and underwriting data*. This consists of information about the policyholders such as how cyber risk is measured, infrastructure, security measures utilised, data stored and processed, and so on. It also includes any loss data on a cyber event or data breach which is usually less than the first set of information. There are other sources of data from private sector firms providing breach data and threat intelligence. Cullen argues [102] though that the volume and depth of data is not available to properly quantify the risk.

Another issue in the quantification of cyber risk is the lack of a common taxonomy. As highlighted in chapter 2.2, we can divide cyber risk into four main areas: (1) the actions of people; (2) systems and technology failures; (3) failed internal processes; (4) external events. Each of these areas is then subdivided into subclasses and each subclass is described by its elements as shown in Appendix IV. Another taxonomy, OCTAVE, developed by SEI, can be used to map tools to controls which are laid out in information security frameworks such as NIST SP 800-53 or ISO 27001. This is useful from an insurer’s perspective in understanding
the causes of risk, and the mitigating actions that can be taken to prevent or reduce such risk, to aid pricing and policy construction.

Security incident taxonomies such as the Vocabulary for Event Recording and Incident Sharing (VERIS), launched by Verizon in 2010 and used to publish the widely read annual Verizon Data Breach Investigations Report (DBIR), is one commercially supported yet public initiative to drive a common threat vocabulary to help build reliable databases in enabling risk carriers to price risk [112]. Other taxonomies available from national CERTs and Computer Security Incident Response Teams (CSIRTs) can also be used [113]. Information sharing schemes such as CISP in the UK also standardises and anonymises threat information [114].

Not only is a lack of data – or reliable data – a major constraint for insurers, but due to the continually evolving threat landscape, cyber risk can be seen as a moving target as new vulnerabilities and attack vectors keep emerging, through for example, zero-day exploits. That said, it seems as though existing and known attack vectors are still being exploited through credential stealing i.e. by using valid login credentials gleaned through social engineering methods to more technical man-in-the-middle attacks [115].

Modelling cyber risk is also key to determining exposure particularly in the area of catastrophe risk. There are three main software and analytics providers (Risk Management Solutions, AIR Worldwide, EQECAT) in this domain and insurers use modelling to calculate loss exposure and risk aggregation among other things. It is important to note that ratings agencies, such as the insurance industry’s A.M. Best, also use modelling to assess insurers. Depending on the insurer’s exposure to catastrophe risk it could impact its solvency ratios and may affect its rating (which in turn could impact its share price, cost of capital etc.) [116].

The lack of data in risk quantification is an important factor in the pricing of policies. A study found [11] that the average pricing of cyber policies was three times higher than general liability insurance and six times higher than property. The variation in available rates in the
market was also much lower compared to other lines suggesting a higher level of conservatism in pricing cyber risk. The combination of high pricing and low differentiation may discourage the uptake of cyber insurance particularly among small and medium sized businesses yet overall demand appears to be strong and capacity isn’t constrained [84].

6.3. Data Sharing Schemes

A Ponemon Institute survey [117] found that out of all technologies available in preventing breaches the single most effective method was through threat intelligence-sharing combined with appropriate technology to help ‘strengthen an organisation’s security posture’. It found an average of 39 percent of all breaches can be prevented as a result of this activity.

As a core component of the UK government’s cyber strategy, the CiSP provides threat intelligence to its members and all insurers can become members and gain access to this resource. Once the National Cyber Security Centre (NCSC) is established by the end of 2016, this could play a centralising role in aggregating that data [20]. The main shortcomings are that the partnership is still in its early days (it was established in 2013) and that incident reporting is voluntary; additionally, not all industries are represented, and, of those industries represented, the larger organisations are dominant.

In May 2016 the head of the ABI called on the UK Government [118] to mandate the reporting of cyber breaches due to the lack of available and reliable data compared to other types of data used for insurance purposes: “we have 350 years of fire data and 10 years of motor and aviation data, but we have just a few years of cyber data.” Whether the UK Government will implement legislation to mandate reporting remains to be seen. Snook argues that: “[Mandatory] breach reporting is not necessarily the right way forward. The key thing to understand is the impact of the breach. You need the quantitative cost” [20].

Yet legislation is on the horizon in the EU (which will also impact the UK despite its impending extrication from the EU) in the form of the NIS Directive [119] and the General Data Protection Regulation [120] which will mandate breach reporting for digital services
providers and operators of essential services and entities controlling or processing the personal data of EU citizens or offering services within the EU (if based outside the EU). Although this mandated reporting will help towards building breach data, it will depend on the type and quality of data reported and will not be industry-wide.

In the US, the financial services sector has been sharing cyber and threat data since 1999 with the establishment of the Financial Services Information Sharing and Analysis Centre (FS-ISAC). This was set up after the 1998 Presidential Directive 63 and later the 2003 Homeland Security Directive mandating the sharing of physical and cyber threat data to critical national infrastructure [121].

More recently, the US Cybersecurity Information Sharing Act of 2015 was conceived to set up a framework for private organisations to share threat indicators or defensive measures, on a voluntary basis, with the federal government. It encourages the use of appropriate security controls to protect this data along with ensuring that any personal data is not divulged and provides protection for participating organisations against anti-trust liability. Although there is widespread support [122] by industry it remains to be seen how successful it becomes, given the potential conflicts of interest between industry and government.

6.4. Implicit Cover or Silent Exposure

One of the main concerns for Lloyd’s is ensuring that cyber exposures are properly quantified by underwriters so that the aggregate market exposure does not conceal hidden or long-tail risk [68] [91]. In order to more accurately reflect the types of exposures and demand from the market Lloyd’s updated its cyber risk code, CY, in 2015 to specifically cover data and privacy breach for first and third-party costs yet exclude damage to physical property. Lloyd’s also introduced a new cyber risk code, CZ, to cover property damage for first- and third-party costs. Lloyd’s acknowledges that the area of cyber coverage is continually evolving and therefore will ensure its approach evolves with it [123].
Another aspect to quantifying cyber risk is understanding the level of exposure of all policies written. Lloyd’s recently asked its managing agents to review their exposure and aggregation risks in both standalone cyber cover and traditional lines where cyber may be covered. There are a couple of important reasons for this: firstly, to capture any exposure explicitly or implicitly made in policies outside of standalone cyber cover; and, secondly, any cyber endorsement offered in these lines will likely have not undergone the same level of risk assessment which is part of the application for standalone cyber cover [91].

Four different types of insurance policies have been identified [89] which could trigger claims in the event of a cyber incident:

(1) a standalone cyber policy: covering first and third-party losses for data breach and property damage as a result of malicious or accidental technology incidents (technology errors and omissions (E&O) liability insurance is a specific line of cover for technology services providers);

(2) a [traditional insurance] policy with affirmative cyber endorsements: this type of policy could be a CGL cover which names a specific cyber peril such as data breach;

(3) a policy with gaps in explicit cyber exclusions: some traditional policies contain exclusions for malicious cyber-attack but permit certain named perils. If one of these perils was itself caused by a cyber-attack this could trigger the policy (CCRS / RMS refer to this as ‘silent cover’);

(4) a policy without cyber exclusions: this could typically be an ‘all risk’ or ‘open perils’ policy in lots of different lines of cover such as property, casualty etc. where loss is triggered by any cause except those specifically excluded [124] (CCRS / RMS again refer to this as ‘silent cover’).

Insurers need to understand their exposure for all risk classes but cyber presents unique characteristics such as its systemic, intangible, and evolving nature that makes it particularly difficult to quantify. Wherever there are grey areas in policies, insurers are likely to face potential legal challenges from its insureds in the event of a disputed claim.
Sony Corporation’s PlayStation Network data breach claim in 2011 was challenged by its insurers who argued that the CGL cover was never meant to cover the actions of [a] third party [hackers]. A Supreme Court of New York ruled in favour of the insurer but Sony and the insurer reached an out of court settlement. Sony’s losses could be as high as USD2 billion as a result of several separate investigations by authorities and 55 different class actions in the US and 3 class actions in Canada [125]. This case demonstrates the risks faced by insurers in having to defend against such actions but equally presents the risks of insureds relying on inadequate or inappropriate policies.

Another issue facing insurers is the ‘long tail’ of cyber risk. This manifests itself in the way that security breaches are sometimes not discovered by insureds until months after the event and after an extensive forensic investigation. This may pose difficulties in assessing whether an insured was covered under the policy at the time of breach yet exclusions and inception date (even if retroactive) in the policy may attempt to address this [126]. Typically, cyber policies are ‘claims made’ meaning an insured can only be indemnified by making a claim within the cover period. Large claims hit insurers during the 1980s and 1990s due to asbestosis and mesothelioma claims made under CGL contracts, some of which dated as far back as the 1940s [71]. These policies were made on an occurrence basis which in effect made them open-ended and unquantified ‘long tail’ risks. Occurrence-based cyber cover has been written but this is generally the exception to the rule [108].
6.5. Accumulation Risk

The head of one of the largest Lloyd’s insurers said after the 2015 Anthem healthcare data breach that cyber risk was the “biggest, most systemic risk” he had encountered in his 42 years in the insurance industry [127]. Aggregation or accumulation risks across different lines of business and different policies is a major concern for the industry.

The pervasive and increasing use of connected information systems and their productivity benefits brings with them associated cyber risks and huge potential economic and insured losses. Insurers calculated the global exposure of cyber risk in 2014 at approximately GBP100 billion (in terms of policies written) of which there is a possible maximum loss (PML) of GBP20 billion for the insurance industry [11].

As part of improving its risk management process (and after heavy losses in the 1980s and early 1990s), in 1995 Lloyd’s introduced an annual realistic disaster scenarios (RDS) exercise to model probable maximum losses (PML) against different hypothetical natural catastrophes. These scenarios have increased over the years and to date there are a total of 16 compulsory scenarios for its managing agents to complete. In 2016 Lloyd’s introduced cyber as a de minimis category for a data breach scenario. Lloyd’s also asked all its managing agents in November 2015 to submit by April 2016 an assessment of their cyber risk appetite compared to risk management processes as well as any exposures across all policies [128]. This should help build a picture of internal or operational risks as well as client risk at the syndicate level and the aggregate risk posed to Lloyd’s as a whole.

In 2015 Lloyd’s and CCRS / RMS published a report [24] on the hypothetical effect of a major cyber-attack on the US power grid. The objective of the report was to highlight three main aspects of cyber risk for insurers (its systemic exposure to all lines of cover, its intangible nature and challenges posed in attributing cause, and the evolving, dynamic nature of cyber threats), shine a spotlight on the risks posed by Operational Technology (OT) used in industrial controls systems (and critical national infrastructure such as power utilities), and estimate the potential insured losses. These ranged from USD21.4 billion to USD71.1 billion.
insured losses out of a total of between USD243 billion to USD1 trillion economic losses to the US economy. To put this in perspective, the capacity of the (re)insurance market for a single catastrophic event is approximately GBP65 billion [11]. This is one of the reasons that certain government backstop mechanisms exist to provide reinsurance in the event of a defined terrorism event: such as TRIA, TRIEA, TRIPRA in the US and Pool Re in the UK [20]. This could be a solution for cyber risk and is being actively considered [102] although opinion is divided as this may dampen the cyber insurance market [20].

CCRS published an earlier report [67] in 2014 outlining a global disaster scenario affecting IT systems in the form of a ‘logic bomb.’ The accumulation risk of computing monocultures raised in chapter 1 is a very real threat to the global economy. We have come to rely on what CCRS terms “Systemically Important Technology Enterprises (SITEs),” that is, companies which produce hardware and software that are critical to business productivity and which if compromised in any way could produce a similar cyber catastrophe to the OT scenario outlined above. In this case however the worst case scenario could cause losses to global GDP of up to USD15 trillion over 5 years.

Zurich Insurance’s chief risk officer equates the potential losses from cyber-crime to the total annual economic losses from natural catastrophes, and says further that “I do not know many companies in peril regions that would not insure themselves against ‘nat cats’. For cyber risks, we all live in a peril region” [106]. The difference between cyber risk and natural catastrophe risk is that the former occurs more frequently and the risk of quantum of loss is potentially equal to or higher than catastrophe risk due to cyber’s global risk profile.

Further studies by CCRS / RMS [89] detail five possible loss scenarios with large accumulation risk: Cyber Data Exfiltration, Denial-of-Service Attack, Cloud Service Provider Failure, Financial Transaction Cyber Compromise, Cyber Extortion. These scenarios are all highly plausible and affect companies of different size, industry, jurisdiction, and activity in different ways. As CCRS / RMS conclude, in order to manage this risk it makes sense to
divide cyber accumulation risk into these categories or segments in the same way as accumulation risk for natural catastrophes is managed, through CRESTA zones.

The Atlantic Council and Zurich Insurance Company Ltd coined the phrase cyber sub-prime in a 2014 report [129]. This equated the sub-prime mortgage debt bubble (comprised of opaque, complex, and highly concentrated, securitized risk) which triggered the 2008 global financial crisis, to a global technology exposure of highly complex and interconnected systems and infrastructure. This carried its own risks, and the report terms this, a ‘cyberization’ of risk which groups seven aggregations of cyber risk: (1) internal IT enterprise, (2) counterparties and partners, (3) outsourced and contract, (4) supply chain, (5) disruptive technologies, (6) upstream infrastructure, (7) external shocks. The report argues that the boundaries between the internal and external functions and activities of organisations have blurred so it is no longer clear where their associated risks start and end, or where new risks could appear.

6.6. Capital Requirements

Babbel argues [130] that the main insurability criteria [79] outlined in chapter 3.1 are only necessary if risk pooling is the primary risk management method used to insure risks. However, what is strictly necessary is that “the insurer have sufficient assets available to honor claims as they arise.” Therefore, insurers, like banks and other financial institutions, need to retain certain levels of capital in order to deal with losses.

Solvency II is a European Directive which came into effect in 2016 with the aim to codify and harmonise European insurance regulation and update risk management practices and maintain capital adequacy levels to a 99.5% confidence level. The Directive comprises three areas, also referred to as pillars:

(1) Financial requirements: the quantitative and qualitative requirements cover harmonised standards to value assets and liabilities and lay down 2 capital thresholds: Solvency Capital Requirement (SCR) and Minimum Capital Requirement (MCR) which set out the amount of capital insurers need to hold to meet its liabilities
with defined confidence levels over 12 months under normal and severe stress test scenarios [131].

(2) Governance, Risk Management and Supervision: Solvency II provides a way to measure operational risk from a capital perspective [41]. A strategy and governance framework needs to be established along with a risk management system which details the insurer’s risk appetite and material risks. This requires insurers to produce an Own Risk and Solvency Assessment (ORSA) to be submitted to regulators. This pillar also details the supervisory process performed by regulators.

(3) Reporting, Disclosure, and Transparency requirements [132] [133]: this addresses how reporting is conducted to the authorities and to the public. Disclosure of risks, risk management, and capital adequacy are required.

The ORSA process is not unique to EU insurers; the US NAIC Risk Management and Own Risk and Solvency Assessment (which went into effect in 2015) came about as a result of the contagion risks to US insurers during the financial crisis of 2008 [131]. The purpose of the annually conducted ORSA is to assess an insurer’s enterprise risk management framework, an assessment of its risk exposure, and its solvency position modelled under different stress scenarios. Cyber risk needs to be part of the risk assessment process and this brings with it all the uncertainty in quantifying that risk.

In the UK, the Prudential Regulation Authority (PRA) has had an interest in the cyber exposure of insurers for at least the past 18 months. Specifically, it is interested in the operational risk of insurers which includes 2 outputs to be delivered by November 2016: internal risk models, and ORSAs. It is surprising to note that, based on anecdotal evidence, some ORSA assessments which have already been submitted, have not included cyber risk [102].

The risks presented to insurers brought about by Solvency II could be in the form of lower competitiveness in the European market compared to other international markets. Solvency II compliance has so far been estimated to cost UK insurers alone GBP3 billion to implement. [134] The practice of ‘gold plating’ (i.e. making the directive more stringent or
conservative) has also contributed to the cost. However, for the London insurance market which specialises in underwriting new and emerging risks, this may only have a marginal impact if it continues to provide such expertise.

6.7. Diversification of Risk

The pooling of risks is central to insurance but it requires those risks to be as uncorrelated as possible. The diversification of risk through different lines of insurance, levels of cover, industries and geographies, and large numbers of policies, should (using the theory of large numbers) bring down the interdependence of the insured risks, and bring estimated losses closer to realised losses. Achieving the balance between covering incurred losses from policyholder claims and maintaining capital requirements, operating costs, and profitability, usually requires investing the premiums collected as well as thorough risk management mechanisms [135].

The primary and excess layers of insurance towers, which may be built up from tens of different entities to meet the capacity required of the cover, also face different risk points. An example given for one USD200 million tower cites 45 different underwriters spanning 27 US markets, 9 in Bermuda, and a further 9 in London each with different risk appetites [136]. The underwriting questions will be shared among all underwriters and the excess layers may have sub-limits of coverage. But this is just another example of how risks can be diversified according to the risk/reward appetite of individual (re)insurers.

The most common method of risk transfer is through the use of reinsurance, sharing the risk of loss by one or several reinsurers for primary or excess cover. If the risks taken on by the insurer exceed its risk appetite, it can choose to share that risk for a fee. Given the tail risk inherent in cyber risk and assuming the capacity is present in the market (there are currently limits on USD500-600 million towers [90]) this diversifies and spreads risks further in the market. Reinsurers will themselves reinsure (through retrocessionaires) as well as use other risk transfer instruments such as Insurance Linked Securities (ILS) which transfer risk to the capital markets.
Catastrophe bonds or ‘cat bonds’ (including catastrophe derivatives and industry loss warranties, collateralised reinsurance, and quota shares and sidecars) are a type of ILS which are issued to provide reinsurance protection to insurers and reinsurers. Cat bonds are issued by investment banks on behalf of insurers to institutional investors keen for higher return investments and to diversify their investment portfolios into an uncorrelated asset class [137]. The ILS market may grow to USD 87 billion by 2019 [77]. Securitising cyber risks in the form of cyber catastrophe bonds is still an untested area, and one which has been argued as an unsuitable mechanism to transfer cyber-risk (as it may give adverse incentives for investors) [138], but the UK government called for proposals in 2016 to investigate ways to make London an onshore centre for ILS for emerging risks such as cyber. This is seen as one important way in leveraging the underwriting expertise of the London market in specialist risk and maintaining its global competitiveness [139].

Similar to bug bounties paid by software vendors, alternative financial instruments such as exploit derivatives may be more useful by incentivising the discovery of unknown cyber exploits in systems to financial pay-out [138]. However, given the small percentage of attacks due to unknown vulnerabilities, it is questionable how popular such investments would be to support a functioning and liquid market.

Re-insurers are also exploring new ways of providing competitive cyber solutions in the market. Munich Re recently partnered with Beazley to combine their respective strengths in assessing and underwriting industrial firms and data breach response and liability to target the largest companies with primary cover solutions [140]. “Primary cover is very profitable, as even though the frequencies of claims are higher, it is much easier to model and quantify the risk. The higher up the tower you go, the riskier it is on the excess side. So although you have lower frequency of claims, you get lower returns” argues Storer of Munich Re [90].

Controlling policy wordings is more a risk-limiter than a diversification of risk. However, open-ended ‘all-risk’ policies or policies which do not explicitly exclude certain perils, can be an unexpected source of risk.
Addressing the systemic nature of cyber, there have been calls for government to provide a back-stop to cyber losses in the event of a catastrophic event, in a similar way as covering terrorism losses. Pool Re was set up in 1993 as a reinsurer to cover losses from acts of terrorism after the bombing of the London Baltic Exchange in 1992. The public-private partnership is owned by its members but HM Treasury guarantees any excess loss over and above the funds available within the mutual. There have been calls to establish a Cyber Re in a similar vein [102] or add cyber cover within Pool Re. Pool Re extended its cover to an ‘all-risks’ basis in 2002 but war and cyber threats are still excluded [141]. This is currently under review [102].
7. Challenges Facing Insureds

In an organisation, insurance as a risk management process can be viewed through the lens of three activities: self-insurance, self-protection, and market insurance [142]. Self-insurance, also known as loss protection, can reduce the size of a loss such as installing fire suppression equipment in a server room; self-protection, also known as loss prevention, can reduce the probability of a loss incident such as installing firewalls and security monitoring systems, or adhering to information security standards and certification; market insurance and self-insurance can be viewed as substitutes, although capital can also be raised and set aside to deal with loss-events. Market insurance and self-protection can, and, frequently are, complementary activities: insurers will attempt to differentiate pricing in the face of information asymmetry challenges (adverse selection and moral hazard) by motivating insureds to self-protect in exchange for fairer premiums [55].

The key starting-point for companies is to treat cyber risk as a key strategic business risk. It needs the support and guidance of the Board and should not be seen as a pure IT risk [82]. Technology systems, data, and infrastructure are business enablers and usually critical to the functioning of most organisations, large and small. The integrity and availability of information systems and the ability to keep systems and data confidential usually run in tandem with an organisation’s business strategy and objectives. Yet in the majority of organisations IT departments continue to shoulder the main responsibility for cyber risk [143]. Armstrong posits [25] that it is critical to treat cyber risk as an enterprise risk; he suggests that the current lack of cyber readiness in some firms is a competitive disadvantage, and even an existential threat. He equates this to the threat posed to Western businesses in the 1970s and 1980s which didn’t invest or re-engineer their processes when faced with Japanese manufacturers’ total quality management systems; the latter ended up disrupting entire industries (such as the car industry).
7.1. How is Cyber Risk Treated in the Organisation?

The holistic treatment of cyber risk is critical in understanding its true impact on the organisation and performing the necessary activities to mitigate and transfer that risk. The Board, risk management, and the finance department are critical stakeholders which all have a fiduciary or financial responsibility and should all be involved in the process. Conducting cyber disaster scenarios and quantifying the impact of a cyber event are necessary even before a decision is made to approach the insurance market [143].

According to an Aon survey, only 59% of organisations which purchase insurance, conduct a formal risk assessment to quantify the limit of cover needed, and almost 50% were unsure whether their organisations complied with international best practices and standards for information security such as NIST or ISO27001. Of those which do purchase cover, one of the reasons stated is to provide “due diligence comfort for the board” [144]. This is somewhat surprising, and suggests that a large proportion of firms are purchasing inappropriate or inadequate cover, but also that cyber risk is not fully understood or owned within organisations.

At Board level, cyber risk needs to be a standing item on the agenda [53] and it needs a multi-disciplined stakeholder approach within the wider organisation where cyber risk assessment, treatment, and ongoing monitoring are an integral part of an enterprise risk management framework and form part of strategy, M&A, and business operations. A security-aware culture should ideally be seen as a business enabler which carries over into the organisation’s relationships with its employees, customers, suppliers, partners, and shareholders. It is as much an internal as an external concern, although arguably, reputational matters may count more as a 2016 Ponemon Institute survey found that: “the biggest financial consequence to organisations that experienced a data breach is lost business” [18].
7.2. Risk Retention, Risk Mitigation or Risk Transfer

In the UK it is estimated that a mere 2% of large organisations and a negligible number (close to zero) of SMEs have purchased standalone cyber insurance, yet 52% of CEOs affirm that they have cyber cover of some form, whereas less than 10% actually do [11]. This suggests there is a large gap in understanding how cyber risk is treated in organisations and what standalone cyber insurance is on offer. In addition, firms which had bought cyber insurance had only done so either in response to a breach or to meet requirements to gain some form of accreditation. These additional findings suggest a reactive or tick-box approach to insurance which tallies with the mainstream view of insurance as a commodity purchase [145].

In the US, the penetration rate is much higher, as evidenced by Table 4 overleaf. A quarter of large businesses (with over USD 5 billion turnover) are estimated to have some kind of cyber cover, yet for SMEs that rate drops to less than 10%. The results from both surveys are largely in alignment.
<table>
<thead>
<tr>
<th>Insured revenue range (USD)</th>
<th>Advisen</th>
<th>Willis Towers Watson</th>
</tr>
</thead>
<tbody>
<tr>
<td>0&lt;500k</td>
<td>2.32%</td>
<td>--</td>
</tr>
<tr>
<td>500K&lt;1M</td>
<td>2.78%</td>
<td>--</td>
</tr>
<tr>
<td>1M&lt;2.5M</td>
<td>3.53%</td>
<td>3.80%</td>
</tr>
<tr>
<td>2.5M&lt;5M</td>
<td>4.93%</td>
<td>4.80%</td>
</tr>
<tr>
<td>5M&lt;10M</td>
<td>5.38%</td>
<td>6.60%</td>
</tr>
<tr>
<td>10M&lt;25M</td>
<td>7.35%</td>
<td>7.20%</td>
</tr>
<tr>
<td>25M&lt;100M</td>
<td>10.76%</td>
<td>10.00%</td>
</tr>
<tr>
<td>100M&lt;300M</td>
<td>19.80%</td>
<td>17.60%</td>
</tr>
<tr>
<td>300M&lt;1B</td>
<td>22.13%</td>
<td>20.50%</td>
</tr>
<tr>
<td>1B&lt;5B</td>
<td>24.35%</td>
<td>21.80%</td>
</tr>
<tr>
<td>5B+</td>
<td>26.63%</td>
<td>25.90%</td>
</tr>
</tbody>
</table>

**Table 4 - Cyber Insurance Penetration Rate**

Source: [146] [89]

A 2016 survey of UK businesses reported that an encouraging 69% of senior managers consider cyber risk as a high priority yet only 51% of companies have taken steps to identify cyber risk, only 29% have formal cyber policies, and a mere 10% have formal incident management plans in place. Again, this suggests that there is a high organisational awareness of cyber risk but little structure or process in place to treat it, and possibly a lack of communication between upper and lower levels of business hierarchy.

As outlined in chapter 2.1 organisations need to decide what proportion of risk is retained and treated based on risk appetite and risk tolerance. *Risk based capacity* and *total cost of risk* are important metrics in determining the appropriate level of self-insurance and risk transfer. Armstrong argues [25] that organisations need to normalise cyber risks; risk mitigation is a relatively narrow activity involving governance and technology. He says, “It’s really a decision about how to deploy capital across the organisation.” Hence, the firm’s cost of capital determines how, and how much, capital is raised in treating retained risk through self-protection or self-insurance measures (by using a captive vehicle), and then deciding what residual risk can be transferred to a risk carrier.

Captives are considered part of the alternative risk transfer market and, as mentioned in chapter 2.1, are insurance pools which are wholly or in part owned (pure or sponsored
captives) by their insureds. According to an Aon Report, 94% of large companies surveyed would share risks with industry peers within a captive [144]. Therefore, an insured puts its own risk capital into a captive rather than use the capital of a third-party insurer. Benefits may include lighter tax and regulatory requirements and the types of risks covered may be wider and have no equivalence in the commercial marketplace; a captive can also be used as a ‘risk incubator’ [147] to better manage and finance the risk; or it can be used for non-standardised or difficult-to-purchase cover such as physical damage, bodily injury and death, or future lost revenue [148]. According to a global Marsh captive report [149] cyber risk liability coverage has seen growing interest in the past 3 years particularly in health care captives as a result of large scale data breaches. However, the number of cyber captives still remains small (20 out of 1,109 or less and 2%) although these may become more attractive to high risk organisations which struggle to find the right commercial offerings.

As described in chapter 2.1 risk mitigation or self-protection (or loss prevention) activities involve people, process, and technical controls. A 2015 report found that of all security technologies deployed, security intelligence systems had the biggest return on investment [5]. Deploying security personnel, appointing a CISO or senior person responsible for security, training and awareness, certification to a standard, and using security metrics, are all critical activities. These may be retained or outsourced to varying degrees but the organisation is ultimately responsible.

However not all risks can be internalised or mitigated and insurers play an important role particularly where the risks may require a certain expertise, where the size of the loss is particularly large but of low occurrence (such as a natural catastrophe), and for new and emerging risks where there is little data, resulting in risks that are hard to quantify (a particular issue for cyber risk) [134].

Once the decision has been made to treat the residual risk and purchase insurance cover (which must include an analysis of existing insurance cover taken out by the firm such as CGL, PI / E&O, and D&O cover), it is important to understand how cyber risk is viewed by different stakeholders in the buying process. A recent SANS and Advisen survey [50]
identified four gaps which organisations need to get to grips with when procuring cyber insurance:

1) The Terminology gap: information security professionals and risk managers within an organisation tend to view risk differently; within the insurance community there is not yet a common lexicon to describe cyber risk. “[W]hen you’re talking to... a CFO or a risk manager – and when you’re talking to a chief information security officer, they think of cyber as two different things,” says one broker [150].

2) The Assessment gap: risk assessments combine qualitative and quantitative approaches. An underwriter would typically favour a more quantitative approach compared to a security professional yet both are at a disadvantage in not having access to historical data; combined with that is the evolving nature of cyber threats which make modelling past events unreliable indicators for future loss events. As such, there may be more need for qualitative assessment by underwriters using expertise gained from other lines of insurance. Commonly used information security frameworks such as NIST 800-53 or ISO 27000 need to be mapped to minimum cyber hygiene requirements set by underwriters to better understand the reasons why underwriters reject cover; for example, defining parameters around terms such as ‘inadequate’ such as ‘inadequate testing procedures and audits.’ Such terms are vague and open to interpretation.

3) The Communication gap: all relevant stakeholders within an organisation must be aligned and involved in a decision to purchase cyber insurance. It should also be a continuous process as risks, lines and levels of cover evolve. Understanding the organisation’s security posture, risk management, and risk financing requires input and coordination from different departments in order to decide on the appropriate level of cover for the needs of the organisation as well as the cost.

4) The Investment gap: most respondents to the survey had to undergo some activities to change their security profile. This may have involved updating policies or adding or updating technical controls. Due to the fact that many cyber insurance policies include (typically for a fee or built into the premium), or provide access to (at preferred rates), ex-ante and ex-post technology, legal, PR, notification, credit
monitoring or other services, along with financial indemnification for a loss event, it may not be clear how much an insured needs to invest in its own self-protection. This raises the issue of moral hazard. But as the survey suggests, self-protection activities could improve the cover offered (i.e. lower premiums) and reduce the likelihood of claims being denied.

Once the organisation has understood its risk tolerance and risk appetite, documented and quantified its overall risk profile, has a risk treatment plan, and aligned the necessary internal stakeholders, it can then choose to transfer a portion of cyber risk out of the business. Some risks may already be covered in whole or in part by existing insurance cover purchased by the firm, so a current state assessment would be necessary before approaching the market. In terms of how the assessment is done, according to a Ponemon survey in 2015, 22% of respondents hired a third party to conduct a formal risk assessment compared to 18% who used internal resources; 20% hired a third party to evaluate policy terms and conditions, and 13% relied on the insurer to conduct the assessment. This last statistic serves to highlight an interesting risk to companies which was raised by a US-based interviewee: an insurer’s due diligence could be used as a roadmap in a possible lawsuit. In other words, an organisation’s internal security profile conducted as part of an insurance application could potentially be accessed in a legal discovery process (as the possible consequence of a breach). So if firms want to avoid having their ‘dirty laundry’ made available, they may wish to use an external auditing firm and put the process under client-attorney privilege [145].

7.3. Lack of Standardised Cover

A commonly held view of insurance is that buyers treat insurance as a commodity. Sellers may also hold that belief knowing that insurance works on the law of large numbers; the objective is therefore to outrun the losses with the sale of policies. But cyber cover typically requires a more specialised approach, particularly when large lines of cover are written. As a result, detailed questionnaires (or questionnaires which ask the right types of questions [84]) eliciting information about the size and type of business, its security profile, value of
assets, and risks posed, along with risk assessments (which may include on-site visits and technical assessments such as pen testing) are standard.

There are a couple of common characteristics with current cyber offerings: the first is that a majority of cover is focused on data privacy (Armstrong states that of the 87 CY designated products, 82 cover privacy and confidentiality of data, such as personal, financial, and health data), the second, is that there is little standardisation of policies. The latter point may explain the slow take-up of standalone cyber cover (excluding regulatory-driven cover). In fact, a Ponemon Institute survey showed that one of the main reasons (31% of respondents) for not buying coverage was a perceived inadequacy of cover relative to exposure. The survey also demonstrated two further issues: the premiums were too expensive (29%) and there were too many exclusions and restrictions, as well as risks that were uninsurable (26%) [151].

So which firms would be motivated to buy cyber insurance? Aside from regulatory compliance reasons, according to one industry respondent [145] there are 2 prime motivators: either the organisation is “ahead of the curve”: it is sophisticated in its risk management processes and it understands the issues, and it understands that even a tailored policy will not necessarily cover all the gaps or areas of residual risk. If the policy does provide cover, the levels may fall below the estimated financial impacts of a loss event, or the retention levels may be high; or secondly “it’s been bitten”, that is, the company experienced a breach and the resultant fall-out.

Another motivator may be the inclusion of additional ‘valued added’ services tied (or as an add-on) to the policy. This can encompass both ex-ante and ex-post services, as described in chapter 5.1. Ex-ante may include online risk management tools but the ex-post services are possibly the most critical, part of the cover [84] and which may be heavily discounted. If less than the equivalent market rate, this could be the main reason firms purchase cyber insurance [93]. It is important to note that while such ex-post services are a critical part of the offering, it may in fact be the ex-ante services where most value is placed: it is usually better to avoid a loss to begin with.
Given the ever-shifting cyber landscape, the lack of data (lack of historical data, variances in taxonomy, and limited information sharing), and the unreliability of existing data to predict future losses, underwriters face a Sisyphean task in quantifying their exposures. Insurers also rely on the insured’s business profile and its risk-weighting will be affected by its industry and business activity, turnover, staff numbers, jurisdictional presence, data stored, transmitted or processed, in addition to its unique security footprint and maturity. [11] There are many different criteria so it is perhaps unsurprising that there is a lack of standardisation of cover. Insureds looking for cover should establish strong relationships with their brokers (this should really be a specialist broker who understands cyber risk) and insurers, and arm themselves with a legal firm which has experience in cyber risk.

Additional challenges in policies are the differences in policy definitions. As the SANS report [50] highlights: “[T]he actual definition of risk assumed under an insurance policy depends on the language in the policy. Two different insurers may think they are covering the same risk, but they may not be because they use different words to describe the risk.” Any confusion in the policy language may result in a claim being disputed in the event of a loss for the insured including the coverage triggers of the policy. There have only been a small number of court cases so far to dispute claims and areas of cover but this may rise as and when claims are made. The report concludes that the courts may be the entities which “shape the cyber insurance industry.”
Understanding the types of cyber risks which are covered by insurance is a critical step in defining the risk treatment of the organisation. As shown in Figure 9 there are certain risks such as death and bodily injury which are unlikely to be covered by a cyber insurance policy or traditional cover; reputational loss is another area which may not be covered in many policies. Figure 8 highlights that less than half of all policies examined had cover for reputational damage. An Aon report found [88] that although reputational risk was its top identified risk in 2015, it was a category of risk which had “insurance design challenges.” Such covered risks may also be constrained in their coverage where an overall policy may have a high limit but each sub area of cover may have low sub-limits or exclusions or necessary retention levels which may make the policy less attractive to the insured.

In fact a majority (almost 95%) of companies surveyed [144] by Aon stated that clear policy wording is the most important issue in the cyber risk market followed by concerns about the loss adjustment process and the willingness to pay claims. This lack of clarity concerns gaps in traditional property and casualty lines and how specific cyber insurance can cover these
gaps. The lack of consistency in cyber offerings manifests itself in the areas such as the taxonomy, the cover limits, pricing, policy triggers, and exclusions.

Organisations which may already have different insurance policies should check whether any of these policies include cyber cover or whether cyber is specifically excluded. Even in the event that cyber is included, the policy limits may not be sufficient to cover the first- and third-party risks which are relevant to the organisation. With all policies the ‘devil is in the detail’. As standalone cyber cover is far from being commoditised it can be difficult for insureds to understand the differences in the various policies offered by all carriers. Therefore, procuring insurance should be a collaborative process between risk managers and security professionals and other necessary stakeholders within the business.

Nevertheless, evidence shows that this is not generally the case as policies tend to be purchased ‘in silos’ [152] which can lead to gaps in cover or provide unnecessary cover for risks which have been retained or mitigated by the business. Given these reasons, and the unique requirements of each organisation (including its security profile and unique threats posed to each industry), insureds must ensure that they develop strong relationships with their broker and insurer(s) to procure the relevant cover.

An example where an insured misunderstood its level of cover (or where it faced an unfavourable court ruling on its interpretation of the cover provided) happened to US fast food chain P.F. Chang’s China Bistro, Inc. in 2014. The company brought claims against its insurer, Federal Insurance Company, following a data breach. The insured discovered that it was not covered for liability for the fees and assessments charged by its debit and credit card processor, Bank of America Merchant Services (BAMS, which in turn was contracted to MasterCard, and in turn liable to fines from MasterCard), as a result of the breach [153]. In the absence of specific Payment Card Industry (PCI) cover in the cyber insurance policy the court ruled that the policy excluded third-party liability to which P.F. Chang’s was exposed via its Master Services Agreement with its acquiring bank, BAMS. As a result, although P.F. Chang’s received indemnity of USD1.7m for the breach from Federal, it was separately liable to pay approximately USD2 million to MasterCard for fees and assessments. This
demonstrates how cyber policies need to be thoroughly examined to check whether each risk relevant to the organisation is adequately covered.

7.4. Attribution and Exclusions

There appear to be large variances in firms’ understanding of their existing insurance cover as opposed to their actual cover, as well as what can be covered by the insurance market [146] [11]. This can be due to a variety of factors but the language of insurance policies is one area of complexity.

Traditional insurance policies may offer limited cover for cyber risk whether implicitly or explicitly and these have evolved over the years to adjust to this new emerging risk class. One example of a widely recognised limit of cover is on contingent business interruption which may either not be covered at all or have strict limits imposed [108] [90]. Exclusions are another method for limiting risk exposure and can be present in all lines of insurance cover. Over the years, as cyber has grown as an emerging risk, various exclusions have been added to traditional lines. In fact, standalone cyber insurance can be viewed as cover which fills in the gaps of traditional lines of cover [154]. Insureds looking for a comprehensive risk transfer solution may need to combine explicitly covered cyber risks either through write-backs (add-ons to traditional policies) or bundling into a standalone cyber cover [11]. It is therefore important to analyse policy wordings for common exclusions which may negate cover [126] along with the stated sub-limits of each different category of cyber risk.

According to the ABI [155], typical exclusions across all lines of cover include war and terrorism events but specific exclusions for cyber policies include the following areas:

1. Court jurisdiction: a business entity may span many different geographies and jurisdictions but a policy may be limited to certain areas or specifically exclude some such as the United States.

2. Claims by related entities: while a professional indemnity insurance (which may be a regulatory requirement for some types of firms) will cover claims from clients it will not usually cover claims from employees. Therefore, a claim brought by a client of
the firm as a result of a data breach may be covered while a similar claim brought by an employee of the insured would typically not be covered.

3. Bodily injury and property damage: typical cyber cover indemnifies against loss or damage to intangible assets. Property and Casualty cover will typically exclude loss to physical assets as a result of a cyber incident. Even standalone cyber cover will rarely include this loss category. Of the types of policies examined in Figure 8 only 19% and 15% of policies covered physical asset damage or death and bodily injury, respectively. This is likely to be a growth area for cyber cover as Operational Technology becomes a more widely-covered sector.

4. Crime versus cyber insurance: as the threat landscape evolves so do the ways in which existing threats are exploited by new vulnerabilities. As the majority of reported UK crime [21] has now morphed into the digital realm into both cyber-enabled or cyber-dependent crime, it is important to distinguish between events such as a data breach (and its accompanying costs and losses), and a fraudulent transfer of funds from a company bank account. Cyber policies typically exclude direct financial loss so the latter event would typically be covered under a separate crime insurance policy. That said, CEO fraud or Business Email Compromise (BEC) scams may equally not be covered, or triggered, by the crime policy [156].

Cyber cover also usually differs from traditional lines of cover in one key area: contracts are almost always written on a claims-made basis rather than on an occurrence or claims-occurring basis (although there are exceptions [108]). Insurance policies are usually written as either type and claims are only paid for the former when claimed during the policy period or when the loss or harm occurred with the latter. CGL policies written more than 50 years ago on an all-risks occurrence basis resulted in huge open-ended liabilities for insurers in the 1980s and 1990s bankrupting many Lloyd’s Names. CGL policies are still written on this basis but will be limited by various endorsements. Organisations seeking cyber cover should where possible negotiate a retroactive start date to the cover in the event of a data breach being discovered during the policy period, but after forensic investigation, learning that the breach happened before the inception of the policy. This is important as a Mandiant Consulting report found the median time to discover a breach was 469 days in 2015 [157].
Figure 10 highlights the areas where cyber risk can be covered in the main traditional lines of cover, and Table 5 provides examples within each line of cover of typical exclusions or negative endorsements. These areas were identified in a 2016 cyber risk scenario report by the International Underwriting Association of London and law firm Norton Rose Fulbright LLP [154]. This serves to highlight that where there are gaps in cover, the purchase of a standalone cyber cover may be the solution.

![Figure 10 - Cyber Risks and Cover Provided by Traditional Lines of Insurance](source: [154])

The Insurance Services Office (ISO) has published a number of cyber endorsements over the past decade for the widely used Commercial General Liability form (an industry standard for general liability cover). Importantly, it specified that electronic data (or software) is not tangible property. Additional exclusions removed cover for unauthorized access to, among
other things, personal financial and health information as well as a range of intellectual property. Property policies can either be all risk policies (subject to exclusions) or named peril policies. Named perils cover, as it suggests, will only cover the specified perils such as loss caused by fire and explosion. The common Lloyd’s exclusions include the Electronic Data Exclusion NMA2914 / NMA2915, the Institute Cyber Attack Exclusion Clause CL380 (typically present in marine and energy policies), Terrorism Insurance Physical Loss or Physical Damage Wording LMA3030 exclusion 9, and War, Hijacking and other perils exclusion clause in aviation insurance AVN 48B (the latter does not explicitly endorse cyber but at least a couple of exclusions such as “(e) and malicious act or act of sabotage” and “(g) Hi-jacking or any unlawful seizure or wrongful exercise of control of the Aircraft or crew...” could apply in a cyber loss scenario [154].

Exclusions can have a wider impact on the enterprise risk management of an insured. One example was raised [90] with CL380, where because cyber is excluded in the line of cover purchased, the insured may technically be in breach of its banking covenants. In other words, where an insured has taken out a loan with a financial institution, the contractual agreement will state various requirements under which the loan is made. This will usually include language stipulating the purchase of adequate insurance cover. Any exclusions in insurance cover, which open up the debtor to potentially large liabilities, may invalidate these conditions. This presents a credible and serious threat to companies with such banking covenants but it also opens up opportunities for insurers to be more creative in their product offerings.

Attribution for a loss is also critical for an insured in making a claim and for an insurer in deciding whether it is liable to indemnify the insured.

“When considering the areas in which cyber exposures may arise and how non-specialist policies may respond, it remains important to have in mind the fundamental principles of insurance law, especially in respect of issues of causation and the application of exclusions. Establishing the cause or source of a loss is vital to
assessing whether any given policy will respond or if an exclusion operates to the insurer’s benefit” [158].

In English law a determining factor is ‘proximate cause’ which refers to the “dominant, effective, or operative cause of the loss” [154]. There may be several proximate causes, particularly as a result of a cyber-attack, which result in a loss and which may determine whether or not an insurer is liable. There are two possible scenarios which determine liability for the insurer: (1) if there are two proximate causes of loss, where one is covered and the second is neither covered nor excluded, then the insurer will most likely be liable; (2) if there are two proximate causes of loss and one is covered and the second is specifically excluded, the exclusion will override the entirety of the loss claimed.

<table>
<thead>
<tr>
<th>Insurance line</th>
<th>Exclusions &amp; Limits of Cover</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. Property Damage &amp; Business Interruption</td>
<td>Trigger for cover is typically physical loss of or damage to property</td>
</tr>
<tr>
<td>B. Aviation</td>
<td>Specific exclusions likely to apply in the event of a malicious or terrorist act</td>
</tr>
<tr>
<td>C. Marine</td>
<td>Specific exclusions (e.g. CL380) likely to apply in relation to ‘computer’ use or an operation as a ‘means for inflicting harm’</td>
</tr>
<tr>
<td>D. IT / Computer</td>
<td>May only cover loss to physical computer hardware</td>
</tr>
<tr>
<td>E. Crime</td>
<td>Trigger for loss is typically a malicious act and monetary loss is often necessary</td>
</tr>
<tr>
<td>F. Employment Practices Liability</td>
<td>Cover only provided for certain types of claim brought by employees</td>
</tr>
<tr>
<td>G. Professional Indemnity</td>
<td>Trigger for cover is usually negligence in the performance of professional services which will not usually cover claims by employees. Cover may often be restricted to claims by clients and not third parties</td>
</tr>
<tr>
<td>H. D&amp;O Liability</td>
<td>Cover is provided for directors and officers and not the organisations they are employed by and most policies will not cover property damage or business interruption</td>
</tr>
<tr>
<td>I. Product Recall / Product Liability</td>
<td>Only covers bodily injury and physical property and not intangible losses or damage such as data loss/modification or business interruption resulting from non-physical loss</td>
</tr>
<tr>
<td>J. Commercial General Liability</td>
<td>Only covers bodily injury and physical property and not intangible losses or damage such as data loss/modification or business interruption resulting from non-physical loss</td>
</tr>
</tbody>
</table>

Table 5 - Exclusions and Limits of Cover in Traditional Insurance Lines

Source: [154]
Attribution for cyber events can be challenging in terms of who did what, and when. Threat actors can be hard to pinpoint, their intentions opaque (a compound attack such as the 2015 Carphone Warehouse data breach started with a denial-of-service attack which diverted attention from the main objective: a data breach [19]), and locating where and when a breach occurred may be a lengthy and costly process. This is no doubt why insurer-supplied post-breach services seem to have incentivised the purchase of standalone cyber cover [93]. Indeed, according to the 2016 Verizon Data Breach Investigations Report the majority of cyber insurance pay-outs go towards the costs incurred within the first stages of a breach recovery. Both legal guidance and forensics account for around half the total costs with breach notification and credit monitoring at less than 20% [19].

Attribution also impacts the policy triggers. This could also be from a loss or claims-made basis. Some policies exclude cover if the attack is deemed to be an act of terrorism (and this attribution may need to be certified by a government source such as the Secretary of the Treasury for the applicability of TRIA). Online groups Anonymous and Lulzsec are classed as terrorist organisations and yet data breaches in 2011 by such activist groups surpassed traditional criminal online activity [159]. There can be a blurred line between cyber-attack and an act of cyber terrorism or how to define whether an event is a result of malicious activity. Additionally, what triggers a cyber incident could be the result of a failure of the insured’s computer system security while a privacy event is a failure to protect confidential information. The first event does not necessarily invoke the second or vice versa. Some carriers may split liability coverage for cyber and privacy events [160].

Of note, any policies which cover the acts and omissions of third parties will only continue to gain in importance given the increasing reliance on cloud-providers in hosting confidential information. Given this growing trend, and where applicable, an insured should specifically aim for a policy which covers data breaches of third parties. In fact, third-party contractual requirements may serve to encourage the take-up of insurance more generally.

Insureds need to be mindful of the issues presented by gaps in cover in traditional lines and standalone cover including the policies underpinning such cover. Policy language and
endorsements can be a minefield to navigate. As one interviewee remarked: “Most [insurance] policies are like Swiss cheese and it takes several to mostly fill the holes” [60].

7.5. Legislative Drivers and Legal Risks

Public disclosure of cyber risks, where they are deemed to be of material importance, is becoming a requirement for publicly listed companies. The US Securities and Exchange Commission released a guidance [161] on cyber risk to public companies in 2011 in line with existing general risk disclosures (Regulation S-K Item 503(c) and Form 10-K requirements since 2005 [162]) to disclose where there are ‘material cybersecurity risks’ to the organisation. Additional disclosures include how cyber risks are addressed, possible costs and consequences of a breach or breaches and breach history (where applicable), and relevant insurance coverage. Willis released a report in 2013 to examine the disclosure of this information in the Fortune 1000 and found only 6% of companies specifically mentioned addressing cyber risk through insurance, although this risk may have been included in other lines of cover [163]. Similarly, in the UK, disclosure of cyber risks should be made where the risks are material. The 2006 Companies Act required companies to describe principle risks facing an organisation and the revised 2014 UK Corporate Governance Code requires Boards to include within the annual strategic report (accompanying the annual report) a ‘robust’ risk assessment and review of the effectiveness of risk management procedures in place [162].

Legal risks for companies come from some of the following areas following a data breach: customers, suppliers, employees, regulators, financial institutions (cards and clearing funds), shareholders against executives (shareholder derivative suits), consumers affected by a data breach (who may form a class and launch a class action suit against the company), investors buying into a company’s stock or existing shareholders affected by a share price drop as a result of a breach, ‘multimedia’ risks from copyright to defamation, and even environmental damage.
In the US, class action lawsuits continue to target breached companies for negligence (in 75% of cases) particularly in the health industry [164]. Although 83 suits were filed in the 2015 period only 21 were against unique defendants, which indicates a trend known as a “lightning rod” effect. This demonstrates the preference of plaintiffs to target multiple suits at companies connected to the largest data breaches. The affected data was overwhelmingly personally sensitive data.

D&O insurance may be a category of cover which sees an increase in demand from insureds [89] as a result of cyber liability claims. However, although class actions are a major exposure for public companies, there have been relatively few successes to date – settlements are more likely [165]. The International Corporate Governance Network (ICGN), an institutional investor group, views cyber risks as those which “can impede the achievement of company objectives and investor returns” [166]. But it is difficult to prove loss as a result of a data breach. In fact, the share prices of affected firms do not seem to suffer over the long term [167], and it is equally hard to prove a breach of fiduciary duty. It is more likely that any D&O claims would come from a shareholder derivative suit which would target the conduct of directors and officers once the cyber-attack had been identified and disclosed, and not the acts and omissions prior to this event [165]. The main take-away for insureds is to have a well-rehearsed incident response plan in place which could form part of a standalone cyber policy.

In Europe, with GDPR effective from May 2018, it seems likely that this will push up demand for standalone cyber cover in Europe. Although it is not clear to what extent the fines are insurable in each jurisdiction [105]. Ellwood also notes [68] that although the onset of regulation will drive demand, there are some jurisdictions which will not permit the cover of fines, and it is also uncertain how GDPR will work in practice. Both GDPR and the NIS Directive have specific breach reporting requirements.

In the UK, a more immediate change to the regulatory environment is the new 2015 Insurance Act (which comes into force on 12 August 2016) which places increased disclosure requirements on business insureds. A key element of the Act is for insureds to disclose
information they actually know along with information they ought to know under the principle of ‘fair presentation of risk.’ This requirement needs to bring together individuals within the organisation who ‘play significant roles in the making of decisions about how the insured’s activities are to be managed or organised.’ The insured now needs to prove that they have carried out a ‘reasonable search’ for relevant information within and outside the organisation and this information should be presented to the insurer in a ‘clear and accessible’ manner. Any material representation of information needs to be ‘substantially correct’ and has to be made in good faith [168]. The complexities of quantifying, monitoring, and treating organisational cyber risk may fit well within the aims of these new legal requirements and should help resolve some of the information asymmetry problems inherent in any insurer-insured relationship. Whether this has any impact on demand for cyber insurance is unclear, yet it may well aid underwriters in their quantification and pricing of risk, which may yield some benefits (such as lower premiums) to insureds.

7.6. The SME Challenge

The current cyber insurance market for small and medium sized enterprises (SMEs) is not as well-developed as the market aimed at larger organisations. Supply may well outstrip demand [20]. Around three-quarters of UK small businesses reported a security breach in 2015 [146] so it may be unsurprising that the latest Zurich SME Risk Index puts technological vulnerabilities as the main threat to the business success of 42% of UK SMEs surveyed. More specifically, cyber-attack and privacy breach at 38% and 37% respectively, are their highest concerns [169].

In 2014 the UK Government launched the Cyber Essentials scheme which was developed in conjunction with the insurance industry to help in underwriting risk in the SME market. The scheme provides a framework of controls across five areas to help organisations achieve a baseline level of cyber-hygiene. It is now also a mandatory requirement for organisations to achieve certification if providing certain services to central government. Half of all firms surveyed recently [10] now state that they have implemented half of the controls in the five key areas but this drops to 5% for firms which have implemented all steps. Only 2% of firms
have adopted the standard. A disproportionately high number of small (63%) and medium-sized firms (66%) outsource their cyber security, although these may just be security services included with an outsourced business offering.

The main cyber risks posed to SMEs, as highlighted in Figure 11, tend to centre around privacy and data loss events and crime and fraud events, which may be manifesting in the form of Business Email Compromise (BEC) scams. Cyber extortion, in the form of ransomware, is another growing threat for the SME market. Given their ‘high-frequency, low-impact’ profile [19] ransomware incidents may become a favoured attack vector for SMEs as the breached organisations are less likely to have sophisticated security, backups, contingency plans, or financing in place.

Cyber insurance adoption in the SME market in the UK has been estimated at less than 2% for large organisations and close to zero for SMEs which is far less than what organisations themselves estimate [11]. This is in large part due to a lack of understanding of existing commercial cover (such as a mistaken belief that cyber cover is included in existing cover) as much as a lack of awareness of what is available from commercial carriers. It could also stem from a lack of communication from insurers and brokers or by not having the right products.
A recent survey [170] found that 85% of UK brokers were not confident in articulating the value of cyber insurance to their SME clients whose top concern was recently identified as cyber risk. CFC Underwriting, which partnered with the British Insurance Brokers’ Association (BIBA) to provide a tailored product for SMEs, found that existing products did not address the main concerns of clients. “Cyber risk is the number one biggest exposure that any of our customers have right now...[and it] is horribly misunderstood and mis-sold by the insurance industry,” said Graeme Newman of CFC Underwriting. “[The firm] had the wrong hot buttons,” explained a colleague, James Burns [84], when they tried to replicate their US successes in the UK cyber insurance market. As a result, the cyber insurance product was more specifically focused towards a cyber-crime policy which may turn out to be more understandable and applicable to SMEs.

As SMEs continue to be targeted by cyber criminals, the heightened awareness of cyber risk should translate into some basic self-protection activity but a larger portion of the risk could be transferred to insurers who will likely continue to evolve and innovate in this segment.
8. Future Outlook

A 2013 McKinsey Global Institute report [171] identified 12 disruptive technologies which by 2025 could have a global economic impact of tens of trillions of dollars. Most of these technologies rely on security underpinnings to unlock their innovative economic potential to protect both the technology and the intellectual property from cyber threats.

These threats will continue to grow in frequency, scale, and sophistication. The challenge for organisations (and government and society in general) is to understand the relevant risks they face by understanding the evolving threat landscape and how this maps to their business. This includes having a thorough understanding of the organisation’s information assets, their associated risks, and the options available to the organisation in how to treat those risks.

The professional risk carriers, likewise exposed to their own enterprise risks, which insure different classes of traditional and emerging risk (such as cyber risk), need to be aware of, and appropriately treat, all their organisational and commercial risk exposures. Many insurance products are commoditised, markets are soft, and insurers are rightly keen to look to new areas of growth. These areas, like cyber risk or certain consequences of cyber risk, may have been uninsurable until recently. It therefore requires insurers to pay special attention in the underwriting of such risks and to look to alternative ways of risk transfer such as hedging or securitisation. One way to achieve the former is for risk carriers to continue to develop their own in-house expertise and to partner with, or acquire, security vendors with specific technology and experience.

Studies have shown [55] that combining self-protection measures with insurance generally promotes network-wide benefits. In essence, this combination raises the overall security levels adopted by interconnected organisations which in turn helps other organisations in a network effect. The benefits of self-protection and risk transfer have been demonstrated. Cyber risk cannot be eliminated but it can be managed. The threats posed to organisations are real and universally applicable. The need for organisations to inculcate a security-aware culture through a robust yet dynamic ERM framework is paramount. As companies do this,
and as insurers continue to develop and innovate in their own ex-ante and ex-post services, insureds and insurers may begin to develop deeper relationships.

As cyber breaches continue to escalate in frequency and severity, a tipping point will likely occur where Boards, senior management, and other stakeholders align on cyber risk. Institutional shareholders, strongly motivated by environmental, social, and governance (ESG) investment criteria, will start to see cyber risk as an outsized governance issue, a new ‘bête-noir’ which could feasibly be linked to executive performance-related pay. [85] Companies will start to find better ways to measure and treat cyber risk as a wider operational risk. Data breach cover demand will grow to meet regulatory requirements but general cyber cover will also evolve more widely to include demand for business interruption, reputational damage, and physical damage cover.

There are currently an estimated 40-50 carriers offering some form of cyber cover. It is conceivable that the product offering could fragment into more specialised lines of cover or become wider and come loaded with exclusions and low sub-limits. However, the consensus view among this report’s interviewees was that the industry would eventually adopt cyber into traditional lines of cover (or remove or revise existing cyber exclusions in such cover) as cyber becomes further integrated into enterprise risk.

Third-party risk is another area which companies need to manage, such as where a supplier or customer may share access to the insured’s network. In many ways third-party risk is just an extension of an organisation’s risk footprint. This could be one area which spurs cover for cyber insurance particularly if companies require, for example, their suppliers to take out insurance cover as a condition for doing business. Contingent business interruption (CBI) cover typically triggers in the event of physical damage at a supplier or customer but is rarely offered for cyber related events. This could also be an area of growth albeit with either restrictive terms of cover or limited capacity.

National and supranational governments will to varying degrees introduce and support public and private initiatives to help increase the resilience of organisations which rely on
the internet ecosystem. After the 2008-09 financial crisis, a number of financial institutions – ‘Systemically Important Financial Institutions’ (SIFIs) – were deemed ‘too big to fail’ and were subjected to additional oversight from regulators. According to a Zurich report [129], similar action might be expected to apply to ‘Significantly Important Internet Organisations’ (SIIOs). The possibility of a “‘Lehman moment’” caused by a cloud provider failure impacting hundreds or thousands of its commercial clients, is a real possibility [67]. Global SIIOs may need to be subjected to stress tests in a similar way to SIFIs in order to help prevent or reduce the effects of global cyber shocks.

Government and industry collaboration also seems likely to continue where their interests dovetail in securing networks and developing deeper understanding of new and evolving threats. Information sharing initiatives will gather momentum aided by new breach disclosure legislation, and controllers and processors of PII will have to demonstrate all necessary controls in place to safeguard such information. Government supported reinsurance pools such as a potential ‘Cyber Re’ reserve may emerge or be deemed necessary in order for the insurance industry to provide the right levels of cover that cyber risk needs. Alternative methods of securitising risk, to transfer risk and raise capital, may help to solve any shortfall.

PwC forecasts [172] a number of areas of change in the insurance market: regulation of cyber security will likely to continue to grow, and there will be an increased focus on consumer privacy. The US already has a raft of state and federal legislation in place covering data privacy and notification requirements. The EU GDPR which comes into effect in 2018 will most likely drive an increase in spending on self-protection measures along with insurance demand. Security spending is forecast to reach USD202 billion by 2021 [95] and the cyber GWP may have reached USD7.5 billion by 2020 [173] or USD20 billion by 2025 [3]. Logically, spending on security will also increase for insurers (86% of US insurers surveyed by the New York State Department of Financial Services indicated their information security budgets to increase over the next 3 years [174]).
A future cyber catastrophe event is a possibility. The potential economic losses mount into the trillions of dollars. Insured losses from a single cyber event could be between USD20 billion to USD71.1 billion [11]. But the more pressing concern is the steady erosion of the economic benefits of ICT brought about by intellectual property theft, or business interruption (such as ransomware or denial-of-service attacks), many of which go unreported. The impact of these events can be reduced by implementing even the most basic security controls. What it requires is a holistic approach to security, an approach which is not defined by compliance, but integral to an organisation’s culture, and supportive of business strategy and objectives.
Conclusion

In this study, an overview of the current state of the cyber insurance market was presented, tracing back to the origins of early types of cover and the trigger sparking its demand, to the risks faced by organisations and the strategies used to treat those risks.

Globally written premiums now total an estimated USD2 billion and could reach USD20 billion by 2025 [3]. There are a number of catalysts which are fuelling demand. Legislation is one of them. The first real demand for cover came about to meet regulatory requirements in the US. This has resulted in the vast majority of cover being written for the US market, although the balance could tip back towards Europe over the next 5-10 years as strict data privacy regulations come into effect.

The cyber threat landscape has continued to grow. Threats and vulnerabilities proliferate and no organisation is immune from attack. The annual global cost of cyber-crime is an estimated USD445 billion. [6] The UK’s National Crime Agency recently reported that cyber-crime now constitutes the majority of total reported UK crime.

It therefore seems likely that this trend may follow a similar path in other economies. It should also stand that as awareness continues to grow, the growing cyber risk will fuel spending on more self-protective measures, combined with risk transfer mechanisms such as cyber insurance.

The main issues facing insurers have focused on a lack of historical data, and a difficulty in modelling existing data due to the evolving nature of cyber risks. Data sharing schemes promoted by government and industry, or within industries, are a starting point but there are challenges to be overcome. The main concern for insurers and regulators is managing and quantifying accumulation risks. These can be managed but require careful attention to existing policies to avoid any ‘silent’ exposures, or explicitly through exclusions and policy limits. These risks go hand-in-hand with risk management practices required by regulators to maintain capital adequacy ratios.
Apart from demand to meet regulatory requirements, cyber cover has been slow to take off. This is evolving though and commercial insurance offerings may well evolve from focusing on data breach response to encompass other areas of risk as a result of a cyber event. These new areas of cover, such as reputational cover, are areas where insurers can offer more innovative products. Insurers can also look to alternative ways to diversify new risks and raise capital through securitisation.

Insured organisations need to have a clear picture of their risks and how risks are best treated in line with a business’s objectives. This can involve some form of risk retention (and which may be required with any commercial insurance), self-protection, and self-insurance measures combined with commercial insurance. Board oversight is a priority and the relevant stakeholders need to be involved in this ongoing risk identification and risk treatment process.

The types of products available to insureds are still heavily skewed towards data breach response and traditional lines may offer limited, if any, cover for cyber-caused perils. Standalone cover, often referred to as gap cover, may not offer the most suitable solutions, or may not be clear what is covered. Where insurers can differentiate their offerings, and which can greatly benefit insureds, is through the value-added ex-ante and ex-post services. These services may be particularly useful for SMEs which have limited resources to manage cyber incidents.

Legal requirements already mean that public companies need to disclose material risks. Where personal data is managed or processed additional requirements (security controls or breach notification) may be required. In regulated industries and companies providing ‘critical services’ these requirements may become stricter.

It therefore seems fair to assume that insurance products will continue to evolve as more capacity and more competition becomes available. Products may start to look more alike and more inclusive of risks as additional loss data becomes available and better ways of modelling cyber risk are developed.
Cyber risks may gradually be subsumed into traditional lines of cover over the next decade. What is needed is a continued study of the threats and impact of cyber risk on enterprise risk management and how organisations can choose to best mitigate those risks.
Appendices

I. Interviewees and Contributors

A range of interviewees was chosen to understand the viewpoints from firms or industry bodies within the insurance industry as well as the views of those outside the industry, either in Government, or those with a view on enterprise risk.

<table>
<thead>
<tr>
<th>No.</th>
<th>Meeting Date</th>
<th>Institution</th>
<th>Contact</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>12 July 2016</td>
<td>Association of British Insurers</td>
<td>Matthew Cullen</td>
</tr>
<tr>
<td>2</td>
<td>30 June 2016</td>
<td>Beazley</td>
<td>Andrew Maher</td>
</tr>
<tr>
<td>3</td>
<td>21 June 2016</td>
<td>British Insurance Brokers’ Association</td>
<td>Martin Bridges</td>
</tr>
<tr>
<td>4</td>
<td>13 July 2016</td>
<td>Cabinet Office</td>
<td>James Snook</td>
</tr>
<tr>
<td>5</td>
<td>20 July 2016</td>
<td>CFC Insurance</td>
<td>James Burns</td>
</tr>
<tr>
<td>6</td>
<td>29 June 2016</td>
<td>Hiscox</td>
<td>Matthew Webb</td>
</tr>
<tr>
<td>7</td>
<td>21 June 2016</td>
<td>Investment Association</td>
<td>Andrew Ninian</td>
</tr>
<tr>
<td>8</td>
<td>5 July 2016</td>
<td>Investor Relations Society</td>
<td>John Golifer, Laura Hayter</td>
</tr>
<tr>
<td>9</td>
<td>21 June 2016</td>
<td>Lloyds Market Association</td>
<td>Tony Ellwood</td>
</tr>
<tr>
<td>10</td>
<td>8 July 2016</td>
<td>Munich Re, Corporate Insurance Partner</td>
<td>Chris Storer</td>
</tr>
<tr>
<td>11</td>
<td>8 August 2016</td>
<td>ValueBridge Advisors and International Corporate Governance Network (ICGN): Corporate Risk Oversight Committee</td>
<td>Brian Barnier</td>
</tr>
<tr>
<td>12</td>
<td>8 August 2016</td>
<td>Wells Fargo Insurance Services, Inc.</td>
<td>Scott Ernst</td>
</tr>
<tr>
<td>13</td>
<td>26 July 2016</td>
<td>Willis Towers Watson</td>
<td>Peter Armstrong</td>
</tr>
</tbody>
</table>

*Table 6 - Interviewees and Contributors*
II. Interview Questionnaire

The following questions are representative of the different range of questions posed to interviewees during the interviews.

1) What’s driving demand for cover?
2) What are the main reasons holding back demand from SMEs?
3) Where do you see the growth in the market coming from? Is it still going to be driven by larger firms or are SMEs starting to take an interest?
4) What’s holding back supply, if anything?
5) What industries or types of business are the ones most likely to seek cover?
6) Do you cover any particular industries which are very high risk?
7) Are there any types of companies or industries which you refuse to cover?
8) How do you quantify cyber risk?
9) Is cyber an attractive risk class for alternative channels of risk transfer or to bring in more capacity? I.e. use of captives or insurance linked securities?
10) Do you see an expertise gap in underwriting or broking?
11) It’s been said that insurers and security practitioners don’t speak the same language. Do you see a disconnect?
12) Are questionnaires for the initial risk assessment sufficient? Does this change or are there additional steps depending on the limits of cover or type of industry?
13) How important are the security firms/specialists you work with in the underwriting process or as part of the overall insurance offering?
14) Do you think insurers are uniquely placed to drive better cyber hygiene practice in companies?
15) How does London establish itself as the leading hub for cyber insurance?
16) How soon are we going to see a commoditisation of lines of cover for cyber or is it always going to be viewed as a specialised risk?
17) One of the biggest issues facing the industry is a lack of data. How important are information sharing initiatives (formal or informal)? Should information sharing be mandated by legislation?
18) Do you think the adoption of GDPR will drive demand for privacy cover as we’ve seen in the US? Or will there be a more holistic approach in Europe where demand will include business interruption, reputational cover etc.?
19) Is Cyber Re or some kind of government-supported back-stop necessary to support the market or will this hinder the market?
20) What are the unique risks for a reinsurer? Is cyber similar to catastrophe cover? Are there any unique risks for a reinsurer?
21) How big an issue is silent cover in traditional lines policies?
22) Who purchases cyber cover? How often does the CIO or CISO get involved in a cyber policy? Is there a disconnect in the buying process for cyber cover?
23) Given the move to cloud-hosted services are there going to be any limits in insuring data which is hosted at a third party?

24) Are suppliers seeing an increase in demand from their clients to take out insurance cover (in addition to all the prerequisite security controls in place)?

25) Due to a lack of standardisation of policies and the various exclusions in traditional cover, companies may find it difficult to choose the right level of cover. In your experience what are the most common exclusions?

26) How do you help organisations understand the value of insurance i.e. the return on investment?

27) Where does capacity need to be to meet the risk/threat level? Currently the maximum seems to be USD500m. Should it be at USD1 billion?

28) Are there any regional differences (North America, Europe, Asia...) in demand for cyber cover?

29) What are the main objections from clients to purchasing standalone cyber cover? Cost? Lack of standardisation across policies?

30) Is the future a gradual move from standalone cyber policies to cyber being a standard part of every traditional line of cover?
III. Interview Transcripts

Interview 1. Matthew Cullen, Association of British Insurers, 12 July 2016

Meeting notes

Cyber is still a relatively new market, and a small market. To put it into perspective, the estimated global written premiums (GWP) for cyber at USD3.5 billion is one third of the UK property market at GBP13 billion. The UK GWP for cyber is approx. GBP120 million (2014) which is a very low base.

PwC forecast the growth of the industry at USD7.5 billion by 2020 and Allianz forecast USD 20 billion by 2025.

Cyber covers two things: financial risk transfer plus wider risk management solutions (ex-ante preparation and ex-post response). In some traditional lines of cover you also have this kind of thing e.g. in kidnap and ransom you will engage specialist firms for hostage negotiation etc.

Most cyber policies are written out of Lloyd’s and now starting to see a trend into the retail space. The Hiscox insurance policy looks almost like a small business cover. Specialist firms are seen as important in the sense that insurers are offering turnkey solutions to try and gain a competitive/innovative edge.

There’s lots of specialist expertise at the higher end but when you move down from the top 5 or so brokers and (re)insurers you quickly get a dearth of knowledge. Not surprising that the recent Airmic survey said that most (85%) brokers were not comfortable pitching cyber to their clients. This is acute in the SME market. There are no retail/personal lines cover yet, although this may come.

The PRA has been interested in cyber exposure for the past 18 months in two areas:

- Operational risk of insurers – 2 outputs are to be reported on by November 2016
  - Internal risk models had to be produced
  - ORSAs produced (some ORSAs did not include cyber risk – which is surprising)
- Underwriting risks – i.e. insurers may not fully understand and quantify the risks they are exposed to

Solvency II requirements could potentially restrain the market given the unknown or difficult to quantify risk. One risk is that this could drive business away from London.

The ABI’s guidance on cyber to date has just focused on SMEs which is a little simplistic but a starting point.

There are 4 main areas of challenge for cyber risk:

1) Lack of data

As the market grows the potential exposure to cyber gets larger. This is not sustainable.

The types of data to which we currently have access are:
- Real-time threat intelligence at CiSP from a handful of sources. Challenges are that it is voluntary, large businesses mainly participating but very low numbers. Industry wants information-sharing to succeed but CiSP is limited in what it delivers (threat intelligence)

- Pricing and underwriting data:
  - this consists of information about the policyholders such as how cyber risk is measured, infrastructure, security measures, data stored/processed etc.
  - any cyber event/breach etc. data. This will typically be less than the first set of information

- Some private sector firms such as Intel provide additional sources of breach data and threat intelligence

There isn’t the volume and depth of data that you need to properly quantify the risk.

2) Systemic risk

Cyber risk is equated to catastrophe risk. It is likely that we will have a major event/disaster which involves the use of cloud computing or commonly used software which results in massive business interruption (or other) across businesses, sectors, geographies.

3) Unintended cover across traditional lines

The PRA (and Lloyd’s) is very keen for insurers to go through all their existing policies to check whether or not there is exposure to cyber that has not been quantified/accounted for. Particularly with the capital adequacy requirements of Solvency II.

4) Low uptake of / demand for cyber insurance

The reasons are many but some key reasons are that the potential insured already thinks they are covered in a traditional line of cover, pricing is too high, lack of awareness of risks

Drivers in the market

Two pieces of regulation will have an impact in the uptake of cyber insurance in Europe:

- GDPR – personal data breaches need to be reported
- NIS – cyber breaches need to be reported (for certain sectors)

Pool Re / Cyber Re

Pool Re was set up in the early 1990s. Reinsurers decided they would no longer reinsurance terrorism which forced the government’s hand into setting up an unlimited back-stop in the event of a terrorist event.

There is appetite within the industry to set up a similar pool: Cyber Re. The consensus is that it is needed and should be done but the question is when is the right time. Matt argues that cyber isn’t yet systemic for the insurance industry if you consider that only 2% of businesses have any kind of cyber cover. If a systemic event happens you have 98% uninsured losses which is borne by society generally.

Initially cyber was not explicitly excluded from Pool Re but in 2015 it was decided that cyber should be excluded. Research is currently being conducted to decide whether or not to include cyber into Pool Re.
**Capacity**
The reinsurance market is currently very soft. The wider insurance market is consequently very soft. There’s lots of capital sloshing around with investors looking for higher than average returns in a generally uncorrelated asset class.

---

**Interview 2. Andrew Maher, Beazley, 30 June 2016**

**Meeting notes**

Beazley breaks down their markets into US domiciled and international markets. The main differences between US and Europe are regulation and different demand requirements. The main market for Beazley is in breach response. The flagship product, Beazley Breach Response, is pitched as a ‘turnkey’ suite of services. It provides a range of services over and above the indemnity, described as ‘breach quarter-backing’.

In the US 47 out of 50 states have data breach notification laws. One of the key Federal laws is HIPAA.

The market has evolved in the US and has seemed to have gone in waves. Retailers experienced a number of breaches typically at point of sale (TJ Maxx, Home Depot, Target). Then healthcare providers were hit (Anthem, Blue Cross etc.). Retailers have since ‘upped their game’ in terms of hardening their systems. So from a data / privacy breach angle it’s no longer such an issue. Their emerging requirement now is for cover from business interruption risks.

Healthcare still suffers from breaches but the emerging trend is ransomware such as Cryptolocker. In 2015 Beazley had at least 40 ransomware incidents (there were more in the first half of 2016). Like retail, this has started to move into the business interruption domain but healthcare is still predominantly about privacy. Healthcare providers are hit by the Office for Civil Rights (OCR) with corrective action plans (i.e. fines). The OCR governs the implementation of HIPAA. Beazley has seen an increase in cases of lost laptops and unencrypted thumb drives. Thinks this could be down to a focus on internal systems at the expense of peripheral equipment.

In Europe, although there are data privacy laws the upcoming GDPR may start to change things. The market demand in Europe is primarily for business interruption cover although breach response is also seeing some demand.

On the question of how contracts are structured and how most if not all cyber contracts are made on a claims-made basis, Andy said he had seen one cyber policy recently which was written on an occurrence basis. He wasn’t sure if this was just to get a competitive edge but thought it was unusual.
Beazley has one of the largest (if not the largest) databases of breach data. This is one of their crown jewels, and on the question of data-sharing, said it would be unlikely this data would ever be shared.

When asked if they would not cover certain businesses or industries, Andy said they would be careful with health information exchanges. These would be covered under E&O policies. There could be massive liability.

When assessing companies, they ensure the right questions are asked depending on the level of cover. The higher the cover, the more is involved from additional questionnaires, phone calls, meetings, even site visits. It’s comparable to a property cover (such as visiting a manufacturing plant). But they don’t have the bandwidth to spend too much time on this. They will put exclusions in their policies to avoid certain risks (e.g. not covering unencrypted thumb drives). Apparently they receive some criticism for this but it means they are up front with their clients and that this possibly helps with moral hazard (i.e. clients know they need to do certain things in order to be covered) and they don’t lose money unnecessarily.

There’s plenty of capacity in the market but it’s about finding the next thing. It could be for example insuring against bodily harm in healthcare machinery. It’s still risky though.

---

**Interview 3.  Martin Bridges, British Insurance Brokers’ Association, 21 June 2016**

**Meeting notes**

Zurich, a leading insurer in the market, conducted a recent survey in the market for SMEs. Cyber came out as a significant concern. Airmic conducted a survey of its members which identified cyber as a primary risk for risk managers of larger firms. Across the board the buying companies have concerns on cyber, and the market is still developing.

BIBA provides a number of services for its members. It has had a cyber liability scheme for a number of years. For smaller brokers, having the confidence to sell a product which is not well-established is a challenge. A broker’s duty is to advise a client on their insured and their uninsured risks. Concurs with findings from a recent Insurance Times survey [which found that 85% of brokers were not confident in articulating the value of cyber cover to their SME clients] that because there is no single policy form in the market then the smaller market may lack the expertise to confidently sell these policies.

One of the challenges with a cyber offering is what do you do in the event of a cyber incident. Bigger brokers can bring in separate expertise for their bigger clients’ portfolios. For smaller-ticket operations there is not enough understanding, or premium, to warrant bringing in third-party advice.

BIBA, the ABI, and Lloyd’s have all set up their own cyber committee working-groups. They are currently looking at the wordings of policies.
BIBA works with CFC underwriting to provide a solution to BIBA’s members. The product has moved on from liability risk to include first-party cover such as business interruption. It’s a compelling product for the SME market.

With evolving products like cyber the broker is the face of the insurance industry. As issues, threats and uninsured losses come along, then they look to close those gaps. The bigger brokers will have more power to negotiate with insurers for extensions in cover.

One of the major issues is that there are a lot of unknown risks and a lack of understanding both with clients and brokers. As claims start to come through then you’re going to have a better idea.

Coming back to the Zurich survey, the major finding is that cyber is a leading risk for SMEs but there seems to be a disconnect between that and an actual demand for cover. It may be similar to the development of the D&O market. For D&O cover there seems to be a lack of understanding at the SME level. There’s general feeling that ‘it will never happen to me’. Although the bigger firms are wiser to the risks. Firms seem to understand property and general liability lines but it’s much more difficult to upsell D&O.

They recently negotiated a flood cover with an insurer and an interesting development was that they were embedding cyber cover. Thinks this is an encouraging development. The limits could be better but it is still a good sign.

---

**Interview 4.  James Snook, HM Government Cabinet Office, 13 July 2016**

**Meeting notes**

The inception of the initial Marsh report was the thinking that insurers can play a key role across the economy. They had done an initial survey of business but this view was not initially shared by the insurance industry. They thought this could apply to businesses of all sizes.

The pricing and valuing risk and incentivising good risk management would help flesh out and support the government’s policy goal for UK cyber strategy.

The purpose of the 2015 Government / Marsh report (on the Role of Insurance in Managing and Mitigating the Risk) was:

1. Raise awareness of cyber risk
2. Raise awareness of the disconnect between what Boards thought they were insured for and then finding they weren’t insured at all.
3. Raise awareness in the insurance industry and the efforts required from the industry

The main issue at the time was that the offerings from insurers were incoherent. Their opinion was that insurers still didn’t understand cyber risks. So a group from GCHQ sat
down with a group of insurers to understand how the insurance industry was valuing risk in their policies. Around 60% of their risks were deemed ‘invalid’ or did not make sense. The conclusion was that the industry did not understand how to value the risks. Lloyds also had concerns about the valuation of risks and made sure that its syndicated members put a cap on the value of their policies.

They came to the conclusion that it came down to a supply and demand issue. For SMEs there was actually more supply than demand and for large businesses it was the reverse i.e. demand outstripped supply. This could be down to a problem in the reinsurance market.

Pool Re was set up in the early 90s to cover the physical consequences of a terrorist attack. They are still evaluating whether or not cyber should be in scope. The main difficulty is the problem of attribution: it is not triggered by criminal behaviour such as organised crime; nor does it apply to acts of war so that would discount nation-state involvement. The bottom line is that it is very difficult to know who actually was the perpetrator in a cyber-attack. Cyber Re could be something even bigger than Pool Re. The main issues are the size of the liability and moral hazard. This applies to insurers and owners and operators. If you insure away your cyber risk, then you don’t have the incentives to protect your network/assets etc. There is no consensus on whether the industry needs Cyber Re. If you hand over a commercial market to the government then the consequences may not be in the best interests of the industry.

Regarding information sharing, there is a lack of data. For CISP all insurers can be members, but reporting is voluntary, and there is under-representation in some sectors. Curiously insurers share data on things like fire and vehicles but not on cyber. Possibly because it is still so new and some insurers see a competitive advantage in keeping that knowledge. With the EU GDPR and NIS Directive, GDPR will address some issues on breach reporting but only when it concerns personal data. The National Cyber Security Centre (NCSC) will play a centralising role in aggregating that data. NIS mandates some reporting but only for certain sectors. Therefore, you don’t get a complete [data] picture with both of these bits of legislation. Breach reporting is also not necessarily the right way forward. The key thing to understand is the impact of the breach and you need the quantitative cost. You also need a strong threat base to help develop one’s own capacity. The NCSC should play a key role for the implementation of the UK’s cyber strategy.

On corporate governance: it’s strange that if the CFO of a public company says he is quitting then he would need to disclose that to the markets as it is a potentially market-moving event. But in the event of a cyber breach that is not mandatory even though a breach could be a market-moving event.

The government is still looking into the right regulatory framework. They do not want to mandate these types of controls but they do want to see the right outcomes. It should be down to the individual companies.

On cyber skills: they do not want to mandate that every firm complies with Cyber Essentials – except you would expect that if you’re supplying government then you would need some
kind of minimum compliance. And it is not a stretch of the imagination to suggest that banks would require some kind of cyber minimum standard if they are going to loan money to a business.

Insurers could use Cyber Essentials as a way to influence their pricing policies. Cyber skills are a key part of the national strategy and there needs to be a minimum level in every profession such as HR, law etc.

London as a centre of excellence: feels that London is recognised as a leader in cyber. London has the specialised underwriting skills. Don’t think that over-regulation is an issue. There’s more regulation in Europe and the US.

Conclusion

We need to look at critical national infrastructure – is insurance going to be a viable option for business interruption because it is a massive liability.

Interview 5.  James Burns, CFC Insurance, 20 July 2016

Meeting notes

In terms of experience CFC were one of the first insurers to cover standalone cyber or ‘hacking’ cover at the end of the 1990s along with Hiscox and AIG. The CFC team is one of the biggest at around 15 underwriters dedicated to cyber. CFC is a managing general agent so they outsource capacity to Lloyd’s. The maximum line of cover is USD40 million. Policies written range from USD1,000 to USD1,000,000+

Evolution

CFC started providing cover at the time of the dot com boom. Once the bubble burst the demand for cover almost disappeared. The type of cover provided started initially with liability cover. So if company A transmits a virus to company B then company A will have some kind of liability protection from company B. Very little liability was actually triggered.

Cyber product moved from third-party to first-party so cover then included system damage at the insured party. But demand still didn’t take off.

Business interruption was added as this seemed a natural thing to cover. Industry already familiar at providing this type of cover for traditional lines. Again demand still didn’t pick up. Then the data breach liability regulations came and suddenly the industry took off. This started in 2003 in California and the industry re-emerged with a bang although it did take almost 10 years for the industry to really gather pace. Cyber cover was suddenly about privacy.
They tried the same approach in the UK but found because of a lack of similarity in regulatory environment and culture (the US has state, federal, and regulatory oversight as well as a litigious culture - for class actions) that this didn’t resonate in the UK.

**BIBA partnership and SME demand**

If you compare the noise levels which are very high to the purchasing levels of cover, there is a disconnect. It’s not really taken off. Having said that the way CFC are pitching cyber cover is to be very specific hence ‘cyber-crime’.

One of the main reasons cyber cover hasn’t taken off as quickly as you would expect is that there is a lot of confusion in the market about what cover is provided. The types of perils covered sound almost academic and not translatable to business needs. Once it is stripped down to a single, easy to understand exposure then it’s an easier sell. Even the US SME market hasn’t taken off. It’s very difficult to get businesses to part with their cash.

As a result, they are now beginning to see increased traction from the industry. They had the wrong hot buttons. The insurance industry hasn’t helped by not being clear what cover is provided. Different types of cover appeal to different customers so Business Interruption isn’t a big deal for SMEs but it will be in manufacturing and with large retailers.

**Future drivers**

They don’t see GDPR as a main driver of demand. Not sure yet whether the UK will be impacted. We already have Data Protection legislation in the UK but never seen the ICO take severe action. Will take a number of losses before this becomes a driver for cover.

**Additional services provided with cover**

Ex-post services are critical to the offering. They have the experience and can do the client hand-holding which is critical in the event of a breach.

Ex-ante services provide some risk management services such as an online platform, training videos (phishing, encryption for mobile devices etc.). There are incentives for insureds to do certain things to reduce their risk profile.

**Risk assessment / applications for cover**

In terms of stipulating more rigorous risk assessments they don’t see this as a good way to do business. They feel as though their assessment process is adequate. There’s no need to engage services of a pen testing firm. It’s a very competitive market.

Will find that other insurers have reams of questions but CFC finds you need to ask the right type of questions to have a greater insight into the risks to be underwritten.

**Standards**
Ideally would like their insureds to have ISO 27001 but it’s a high bar and not many firms will have this.

However, if you’re based in the US and you store and process health care information then you would need compliance with HIPAA. So this would be a red line.

For PCI if you’re storing, transmitting or processing card-holder data they would expect PCI compliance in 99% of cases or a very good reason not to have compliance.

**Risks**

The main risk is aggregation. There’s a lack of historical data and it’s a competitive market so no real incentive to share data. That’s not unique. Other lines such as professional liability loss data aren’t shared. Fire and auto may be shared on personal lines as there is a greater incidence of fraud so there is more incentive for insurers to share data.

There are a number of market providers such as Advisen and NetDiligence which collect data.

**Capacity**

Capacity is increasing exponentially. They have heard that just in the past 6 months there is additional GBP80 million in the London market.

**Future Outlook**

The future is all about growth. Currently at USD2 billion with projections from USD10-20 billion in the next 10 years.

Exclusions – see some lines of cover where cyber is specifically excluded such as marine and terrorism. Think this will/should change. Cyber cover deals primarily with intangibles so would expect a property line to eventually include cyber as standard.

---

**Meeting notes**

**Market demand**

There are 3 main areas which are driving demand:

1. Boards are generally more aware of cyber risks and the need to transfer some of that risk away from the business;
2. Media coverage of hacking events (‘hacks love a hack’);
3. Regulation such as GDPR
Finds that the level of cyber awareness varies greatly from company to company although as a general rule SMEs are less well prepared than larger firms.

**Hiscox offering**

Hiscox provides both 1st and third-party cover. In terms of third-party cover they will generally cover regulatory fines in privacy breaches. This includes ICO and PCI fines (up to 500k). No precedent to say the ICO fines are insurable but will ‘endeavour to pay these’

**Risk exposure**

Cyber is seen as ‘the greatest opportunity but also the greatest threat’ to Hiscox. Their US business has already seen a doubling of business in 2016 compared to 2015.

Hiscox is currently reviewing their exposure and aggregation risks in 2 areas:

1. Standalone cyber cover
2. Cyber that lies within existing lines such as Kidnap and extortion cover. Eg they may have included cyber extortion as part of the cover without having done a full risk assessment which they would normally do on cyber lines. So it could be explicit cover OR it could be silent cover. Both are big risks. This is particularly true for cyber extortion given its growing importance.

**Risk aggregation**

The main ways Hiscox seeks to control aggregation risk is through policy wording and reinsurance. These are the main risk mitigation controls. If they see an opportunity to offer higher lines, then they would seek to partner with other underwriters to share the risk and business

Lloyds asked the market to submit 3 disaster scenarios for cyber. Hiscox had already been working on these to measure their aggregation risks so ‘was well ahead of the curve’.

**Partnerships with security firms/specialists**

These are key to providing ancillary services such as pen testing, breach response, forensics (e.g. KPMG), legal advice (Pinsent Masons), etc.

---

**Interview 7.  Andrew Ninian, Investment Association, 21 June 2016**

---

**Meeting notes**

Investors engage with Boards on a range of issues from financial performance to strategy to risk. Cyber is clearly a key-risk issue and is high on the radar at the moment. Cyber oversight
is a Board issue. But investors only expect companies to report on cyber if it is deemed to be a material risk – otherwise, no compulsion.

The IA doesn't favour compulsory reporting as this will relegate Board engagement to a compliance issue. The believe this will reduce the quality of the reporting and will reduce the importance of cyber as a key business risk. As soon as it becomes a risk and compliance issue it doesn't have the same Board visibility and level of priority.

They engaged with a UK financial institution recently who told them that they have thousands of breaches every week. That doesn't mean that they are material breaches i.e. that anything was stolen or damaged. These are contained. But how do you interpret that? And what would that mean if you had to report all breaches?

Issues stem from the lack of a framework - although the UK government's Cyber Essentials programme is a starting point. Are investors asking the right questions? What do they do with the results? There are so many different variables.

The types of responses from Boards on cyber risk varies considerably. Another example of an engagement was where an investor asked for a report on the portfolio firm's cyber risk profile. What they received was incomprehensible as it was entirely technical. This is a possible indicator that cyber risk hasn't been fully assumed as a business risk and hence owned by the Board if it can't be communicated in a non-technical way.

---

**Meeting notes**

The IRS has hosted an annual seminar on cyber issues since 2014 and cyber has been raised at other IRS-hosted events and come up anecdotally. The society plans on incorporating cyber into their policy and currently looking into this. The issue of cyber has generated interest but the evidence so far seems that investor engagement with IR professionals is just beginning.

An annual investor relations survey conducted by financial PR firm, Citigate Dewe Robertson, has for the first time raised cyber as a new topic for discussion between investor relations officers and their investors. Based on the survey results 37% of investor relations officers (IROs) are addressing cyber concerns. Of the 37% only 7% of IROs are “fully engaged with investors regarding cyber security arrangements at their companies, whilst another 30% say they are ‘somewhat’ engaged on the issue.” This number seems surprisingly low given the focus on cyber security at Board level. The report makes the observation that “Going forward, we expect investment attractiveness of companies with inadequate policies or systems in place to prevent breaches to diminish as investor scrutiny of their preparedness increases.”
Meeting notes

One of biggest threats in cyber market is not the cyber loss per se but the company’s share value through having been hacked, value of that business having being affected through identity theft, data loss. That can ultimately affect the share price. You can end up with shareholder actions against the company for failing to secure the data. This would come under D&O liability. Arguably, that’s a bigger loss than you ever get under a privacy breach.

As a result of a lot of thefts of data particularly in the US, the regulators got agitated, very demanding in terms of notification, fines and penalties. So the standalone cyber products started to move away from professional indemnity policies. This then became a standalone cyber-breach response policy which shifted the emphasis a little. It still is very much written on the basis of a liability policy but what has started to develop is cover for credit monitoring and restitution. Which made it more of a first-party product.

That in turn has developed into a package. Whether it’s a breach event, notification costs, lawyers, reputational harm, business interruption. You get a cross-over of more traditional areas of cover. If a factory burns down or can’t trade for 12 months because you’ve lost your stock that’s a standard risk that the industry understands. That has morphed over to a certain extent into cyber products. But a website coming down or a server being attacked is not the same animal in the sense of time. Cyber is far more immediate. If someone took down Amazon, then you’re looking at hours. A classic example is [UK company] Talktalk. They ended up losing a lot of customers. Is that a permanent effect on their business? Is that insurable? It’s a complex issue.

Something else we have seen in terms of coverage. Contingent business interruption. If you have a supply chain. If your business relies on a third-party provider, then what happens if they get hacked? Whether it’s an IT issue or your workforce has gone on strike at your factory, the consequence is the same. It’s simply the cause that is different.

As such, cyber is not really a new risk to the industry. It is just emerging in different ways. It has a different look and feel. We may find in 10 years’ time that where you have a traditional property policy which covers fire, flood etc. then why not have it cover cyber as well? It’s only another peril.

A standard cyber policy today is going to exclude (on a breach-response side) physical damage and bodily injury. Those outcomes are excluded. And that gives a distinction between a cyber policy and a traditional property policy. Very little property business written but 2 examples which are often cited are Stuxnet and Iran and the Saudi Aramco hack. Other than that there are very few examples. But these are areas of concern for Lloyds in terms of risk aggregation.
But we struggle to find correlation between privacy events. Exceedingly difficult to measure. If Barclays gets hacked, TalkTalk, and Target and if you’re writing all of those risks (or a proportion of) how do you measure that accumulation? Am I going to suffer a loss all at the same time. Unlikely. But as the business grows the challenge is more to the physical damage side of things. You don’t want it aggregating with other risks. How do you measure 2 separate cyber risks you have written e.g. one in the US and one in the UK? Where are the shared touch-points that allow you to measure the accumulation and exposures?

If you have a terrorism event, then you have TRIA and Pool Re backstops. But how you factor cyber into that is difficult. If the industry is not looking for that cover/safety net then does it need to be provided? Or conversely is the lack of that facility holding us back?

Cyber cover is growing fairly reasonably but predominantly in the US. Their demand has been led by regulators. US on a federal level is reluctant to mandate anything. Driven on a state level. Global cyber premiums are 1.5-2.5 billion. But should get to 20bn soon.

GDPR: not clear how this will work. Outlawed in some EU states for insurers to pay fines. Onset of regulation will definitely drive demand though.

Cyber standards: The Government is looking to Insurers to lead the charge to improve cyber security. Bit of a rocky road. If insurers mandate certain level of cyber security as a precondition – and the expectation is that will bring down your insurance premium – that is a dangerous game to play. Cyber Essentials has a very low common denominator. Simply getting across that line might not be sufficient for an underwriter to accept that risk anyway.

It’s true that insurance does impose some minimum standards but it’s no different to refusing fire cover if you don’t have sprinklers in your warehouse.

Partnering with specialist firms: on two levels. One is where you have the likes of a cyber specialist underwriter which will provide a number of services around breach response which could involve forensics, legal advice, credit monitoring etc. The second is the underwriting process where an insurer may partner with a pen testing firm as part of the initial assessment. But that is not unusual as part of the [general] underwriting process except that it is probably far more technical. Also the problem is that cyber-crime is a moving target.

Is there much sharing of modelling information? No. The managing agents of syndicates would have their own models and they are all looking to monetise what they have. Lot of people looking to get into the space of data capture: record losses and cyber incidents with a view to monetise that.

Sharing of risks – that’s what Lloyd’s does. You can have a 20 million [pound] line of which you underwrite 5 million, and then syndicate the rest. Where it gets more complicated is if you’re the reinsurer as then the risk can become concentrated.
There’s little evidence of a lack of capacity in the market and a lack of innovation contrary to what Airmic has claimed. At the end of the day it’s a supply and demand market. The exception may be if you’re looking at critical infrastructure. Maybe there is a lack of capacity there.

**Interview 10. Chris Storer, Munich Re, Corporate Services Partner, 8 July 2016**

**Meeting notes**

At least 80% of the book is still from North America. The demand has come almost entirely from the regulatory environment with regards to state breach-notification laws.

There isn’t the sophistication in other markets although this is changing rapidly, particularly in Europe. In Asia they have seen some interest but insurance is still seen as a commodity market and cyber risk is not seen as a strategic business risk.

There are more fit-for-purpose solutions in the US. There has also been a steady increase towards business interruption cover from pure data breach cover which is an interesting development. It’s possibly an indicator of a maturing market.

There are five business lines at Munich Re. One of them covers special enterprise risks which is where the cyber line was born. Their speciality is a focus on industrial clients with industrial control systems and OT. It requires a different type of expertise: in the underwriting team but also supported by a team of engineers called ‘Loss Control Engineering’. So although they do partner with many specialist firms they also focus on growing their own in-house expertise.

There are 2 different types of reinsurance:

1) Treaty reinsurance – book of business by cedent across a number of lines – a portfolio
2) Facultative insurance – single line of business

Each reinsurance client will have a cap in the cover they receive. The reinsurer will also dictate the terms in the cover that is given to the end client. Sometimes there is a disconnect in what is covered e.g. terrorism. Does terrorism cover cyber terrorism? In a lot of cases it does, but not always.

Currently there are limits of about $500-600m towers. Chris thinks this is under-priced. He thinks one of the main issues is that good risk is over-priced and bad risk (i.e. what is difficult to quantify) is under-priced.

Some areas they will not cover or apply limits such as on contingent business interruption.
There are also some gaps in cover such as silent cover, that is, not explicitly covered or not explicitly excluded.

Munich Re has identified an interesting opportunity in exclusions on the London market. These are typical exclusions for marine and energy. Cyber is excluded on these. (One exclusion in particular is CL380). That means a lot of companies could be defaulting on their banking covenants because they don't have insurance cover.

ILS and alternative capital is attractive and will continue to grow in the area of cyber.

The recently announced partnership with Beazley is interesting as they are combining their strengths: Munich Re in the industrial area and Beazley in the corporate space. They are targeting the largest firms to provide primary cover. This is very profitable, as even though you have higher frequencies of claims, it is much easier to model and quantify the risk. The higher up the tower you go, the riskier it is on the excess side. So although you have lower frequency of claims you get lower returns.

Overall there could be more cyber expertise on the broking side of the business.

---

Meeting notes

On cyber and the linkage with enterprise risk:

- For some organizations it is linked – when both cyber risk (including IT investment portfolio, programme / project management, and operations stability, availability, recoverability and InfoSec) and enterprise risk are addressed using audit / control / compliance methods. However, those are terrible techniques for managing the dynamic form of prospective or future risk. Recall that audit and controls were designed for managing the risk of accurately reporting the financial consequences of activities that occurred in the past, e.g., expense account or sales reporting.

- When they are not linked – this is when cyber risk (defined as above) is following an audit approach and the business is using more systems / root cause / quality approaches for enterprise risk. However, in this case enterprise risk is managed better.

Using a system/root cause/quality approach is ideal as this is both more efficient and effective for managing individual risks, and is more efficient and effective as the same basic approach is consistently used for all types of risk upon which achieving business objectives depend. This is powerful for another reason. System/root cause/quality approaches have historically been designed to be more simple as that is required for effectiveness in a more dynamic environment (think sports or aviation). A complex approach (as often is the case in control/compliance-based
On top of a complex and changing dynamic environment, tends to increase risk – the opposite of the desired objective.
- There are also other combinations.

On managing risk and risk transfer:

- From a managing risk perspective, we couldn’t care less about insurance for 3 reasons: 1) the risk can’t be transferred, just some of the financial consequences, 2) most policies are Swiss cheese and it takes several to mostly fill the holes, and 3) most insurers have a limited understanding of technology so underwriting is often done from a compliance perspective (that has the potential to increase risk by distracting resources and measurement efforts from actually managing risk). On top of this, the insurance model of accept, reject, transfer and mitigate has confused many companies trying to actually manage risk. The people in organisations responsible for buying insurance, buy what they want (with little understanding of what they are buying) and it has little effect on the actual management of risk. The exception seems to be in event-driven IT disruption where the event can be directly tied to physical needs to switch to alternate locations and such.
- After having taught thousands of risk managers and auditors through ISACA and IIA, I’ve never found one who had sufficiently reviewed the limitations of their insurance policies and sought to improve them. Maybe 5% have some level of review of cyber (defined above) disruption polices, but as soon as I ask a few specific questions, it is clear that their opportunity to deeply review coverage, and/or their subject matter knowledge, was limited


Meeting notes

The US market is much further along from a cyber insurance perspective than other markets. There isn’t a lot of appetite in the UK yet.

Events such as the Target and Sony breaches jumpstarted the market, the regulators turned up the heat, and now companies are spending a lot more money.

The market originally started with 3 carriers including AIG. Now there are around 40 carriers providing first- and third-party cover. In addition, carriers are providing first-response cover which includes breach notification costs, legal costs, credit monitoring for breached customers, loss mitigation services.

Expect to see D&O pop up suits claiming executives of companies failed through lack of supervision and fiduciary oversight of the Board. The current drum-beat in the US is that it’s no longer sufficient for a CISO to be brought on to be the fall guy. Firms need risk management plans in place. The SEC is getting more involved in this.
For larger companies such as Fortune 500 you can throw 30 staff at this problem but for SMEs the difficulty for them is knowing where to start. Lots of firms are trying to do more with less resources.

Regarding broker expertise this is the weak link in the distribution channel but there’s lots of education going on. There are a number of really well-informed insurers and brokers but it’s not what it looks like in other forms of cover. ACE is an insurer with 15 years of claims data [in cyber] and they’re desperate to get that out to the market place but they’re struggling to get that information out to potential buyers.

One of the issues with insurance is that buyers treat insurance as a commodity. Sellers also have a similar mentality in that insurance works on the law of large numbers hence you want to write as many contracts as you can – a ‘plug and chug’ approach. And hope that you outrun the losses with the write.

Cyber cover usually brings with it a more specialised approach particularly when large limits of cover are offered. Insurers may require insureds to follow certain security frameworks etc. They’re keen to see policies and procedures in place, training for employees, an incident response plan.

For pre- and post-services, the insured may be required to use the insurer’s recommended partners.

One reason for insureds to be very wary about the insurance due-diligence process is that it could be seen as a roadmap for a lawyer to use in court. An organisation’s internal security profile conducted as part of an insurance application could potentially be used in the discovery process. If firms don’t want this dirty laundry to be available, they may wish to use an external firm and put the process under attorney-client privilege. Astute companies do this.

If you have already cyber insurance, then you’re 1) either sophisticated and know the issues or 2) you’ve been bitten (breached) and realised you needed it. But it doesn’t always cover all the gaps. A media company is very different to an airline: downtime / business interruption for an airline is catastrophic. Both the attack and exposure vectors are different. Another issue is the policy wording. A term like ‘reasonable security’ can be widely interpreted.

An interesting statistic is that 47% of incidents came through 3rd party contractors. Were these events malicious or accidental. That can matter. [attribution]

Another example is imposter fraud. Wiring money to a dummy account is not a typical crime as defined. This throws up new insurance covers which have not yet been tested.

Policies are a little like the game ‘chutes and ladders’ (snakes and ladders). And as a result of that law suits are coming. Anderson Till is one large law firm which sues insurers.
Information sharing – a couple of the big insurers like ACE and Beazley have years of claims data but they won’t share this. It’s a critical asset. Lots of calls now to share breach information from both the public and private sectors but it’s still at an early stage.

Who buys insurance? The process is like trying to herd cats. In a large firm it could be the risk manager and more people are involved. For SMEs it may be stuck in finance and the insurance application may never have involved anyone outside finance such as risk and compliance or IT or security. Therefore, in some cases an insured may not know what they’re buying.

Corporate should be aware that ratings agencies will start to factor in network security and privacy issues into their debt ratings.

When potential insureds go looking for cover they need to firstly understand their own risk profile. Ask questions about their business, their assets, the potential threats to those assets, understand their exposure. Then they can go out to the market and see what’s available. And preferably ‘lawyer-up’ to understand the policies.

---

**Interview 13. Peter Armstrong, Willis Towers Watson, 26 July 2016**

**Meeting notes**

In terms of products in the market there are 87 with a CY (Cyber) designation. About 82 of them cover privacy and confidentiality of data (personal, health, financial). The cover is mainly from a CIA (confidentiality, integrity, availability) focus. Only a small handful of products would be applicable to an OT perspective. With industrial control systems we don’t care as much about confidentiality – to some extent. Integrity and availability are more important. There are only a handful of insurers who recognise the difference.

The capacity is too low in the market. USD500 million is irrelevant when you have retention levels of USD1 billion (which is what a corporate such as BP would have).

Organisations need to normalise the risk. Cyber risk is not a techy / geeky thing. It’s all down to enterprise risk. It’s not just about risk mitigation which is just about governance and technology. It goes much wider in that it’s really a decision about how to deploy capital across the organisation.

**Key questions Boards need to ask:**

1) Do we understand our cyber vulnerabilities?
2) How are we quantifying our incremental exposure to cyber risk?
3) How do we quantify differential exposure?
Why don’t Boards treat cyber risk more seriously?
1) Cyber is viewed as a single discretionary risk.
2) Margin performance is increasingly challenged at the cost line. Businesses are becoming increasingly digitally-enabled. The problem is people don’t understand technology or its implications.
3) The tech community doesn’t know how to translate the technology requirements, risks, costs, threats and translate that to enterprise risk.

Cyber cover has gone from being a specific product with a specific purpose. What we may see in the future is the category grow massively or just fizzle out. Why the latter? One would expect cyber to be included within traditional lines such as P&C. You wouldn’t have the various exclusions such as CL380 or LMA3030. Cyber would be automatically covered. And that really is what should happen.

If you assume cost of crime is 0.8% of GDP if you just take a linear (as opposed to exponential) approach to its increase by 2020 you could potentially have 4.7% of global GDP in losses attributable to cyber-crime. That’s enough to qualify as a global recession. You have an existential risk to corporates.

The issue is similar to the issue of total quality management (TQM) systems in the 1970s and 1980s. Western companies which didn’t invest, faced the threat from Japanese TQM.

It is critical to treat cyber risk as an enterprise risk: documenting the proof of quantified disclosure, improving of cyber defences, reduction of cyber risk.

In risk transfer, cyber insurance is just one of the levers.

Currently there is no legislative imperative and there is an over-arching problem which is a lack of education and awareness of cyber risk.

Exclusions

Specialist cyber cover will continue to grow or fizzle out. This depends on whether / when cyber is integrated into other lines of cover and exclusions such as CL380 go away.

IoT will bring with it a need for cyber resiliency all along the value chain. Peter gave an example of an airbag manufacturer at one end of the chain incorporating defences into the airbag mechanism and at the other end Deutsche Telecom providing the connectivity to the car/car manufacturer who also has a duty of care to incorporate security. This should help improve the quantification of cyber risk.

Captives

Some firms are winding up their use of captives, as the tax incentives are less of an inducement. However, it may be worth reconsidering and using captives to transfer a
portion of the residual risk. Could have significant role to play. You can then take this off the balance sheet.

If you take the example of the German blast furnace which suffered losses of 6x what it had put aside (40m euros as opposed to 240m euros) in 2015 following a fairly rudimentary attack that’s the equivalent of a company’s pension fund liabilities. Seeking a line of cover either through self-insurance or through risk transfer in cyber cover may not be cost or strategically efficient. You could however use the capital markets and issue debt at 50 basis points for 1 billion and that becomes a much more efficient use of capital. You can then invest in cyber defences and maybe also take out certain insurance cover.
IV. Categories of Cyber Risk

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
<th>Elements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1. Actions of People</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1. Inadvertent</td>
<td>unintentional actions taken without malicious or harmful intent</td>
<td>mistakes, errors, omissions</td>
</tr>
<tr>
<td>1.2. Deliberate</td>
<td>actions taken intentionally and with intent to do harm</td>
<td>fraud, sabotage, theft, and vandalism</td>
</tr>
<tr>
<td>1.3. Inaction</td>
<td>lack of action or failure to act in a given situation</td>
<td>lack of appropriate skills, knowledge, guidance, and availability of personnel to take action</td>
</tr>
<tr>
<td><strong>2. Systems and Technology Failures</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.1. Hardware</td>
<td>risks traceable to failures in physical equipment</td>
<td>failure due to capacity, performance, maintenance, and obsolescence</td>
</tr>
<tr>
<td>2.2. Software</td>
<td>risks stemming from software assets of all types, including programs, applications, and operating systems</td>
<td>compatibility, configuration management, change control, security settings, coding practices, and testing</td>
</tr>
<tr>
<td>2.3. Systems</td>
<td>failures of integrated systems to perform as expected</td>
<td>design, specifications, integration, and complexity</td>
</tr>
<tr>
<td><strong>3. Failed Internal Processes</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.1. Process design or execution</td>
<td>failures of processes to achieve their desired outcomes due to poor process design or execution</td>
<td>process flow, process documentation, roles and responsibilities, notifications and alerts, information flow, escalation of issues, service level agreements, and task hand-off</td>
</tr>
<tr>
<td>3.2. Process controls</td>
<td>inadequate controls on the operation of the process</td>
<td>status monitoring, metrics, periodic review, and process ownership</td>
</tr>
<tr>
<td>3.3. Supporting Processes</td>
<td>failure of organizational supporting processes to deliver the appropriate resources</td>
<td>staffing, funding, training and development, and procurement</td>
</tr>
<tr>
<td><strong>4. External Events</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1. Hazards (Catastrophes)</td>
<td>events, both natural and of human origin, over which the organization has no control and that can occur without notice</td>
<td>weather event, fire, flood, earthquake, unrest</td>
</tr>
<tr>
<td>4.2. Legal issues</td>
<td>risk arising from legal issues</td>
<td>regulatory compliance, legislation, and litigation</td>
</tr>
<tr>
<td>4.3. Business Issues</td>
<td>risks arising from changes in the business environment of the organisation</td>
<td>supplier failure, market conditions, and economic conditions</td>
</tr>
<tr>
<td>4.4. Service Dependencies</td>
<td>risks arising from the organisation’s dependence on external parties to continue operations</td>
<td>utilities, emergency services, fuel, and transportation</td>
</tr>
</tbody>
</table>

Table 7 - Categories of Cyber Risk

Source: [38]
Bibliography


insurance implications of a cyber attack on the US power grid,” 2015.


[53] Marsh and Oliver Wyman, “Making the UK financial and professional services more resilient to cyber attack,” 2016.


2016.


[137] Swiss Re Capital Markets, “What are Insurance Linked Securities (ILS), and Why Should they be Considered?,” 2012.


[169] D. Hunter, “Cyber attacks are the biggest threat to small businesses,” freshbusinessthinking.com, 2016. .


