enisa
European Network and Information Security Agency

Incentives and barriers of the cyber insurance market in Europe

June 2012

Acknowledgements

This Study was commissioned and managed by ENISA with specialist services provided by RAND Europe. ENISA would like to thank Mr. Neil Robinson for his professionalism and dedication to this project.

In addition, ENISA wishes to acknowledge and thank Prof. Robin Bloomfield of City University of London, Mr. Andrea Renda of CEPS, Mr. Michael Mainelli of Z/Yen, Mrs. Simona Cavallini and Mr. Fabio Bisogni of Formit Foundation for their prompt support, valuable input and material provided for the compilation of this Study.

About ENISA

The European Network and Information Security Agency (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu

Contact details

For contacting ENISA or for general enquiries on this Study on cyber insurance market in Europe please contact Nicole Falessi and Dr. Konstantinos Moulinos and use the following details:

Resilience and CIIP Program
Technical Department
Email: resilience@enisa.europa.eu

Contents

GLOSSARY

CYBER-ATTACK – includes a wide range of technical and social methods to pursue an ultimate goal – the propagation, extraction, denial or manipulation of information[1]

CYBER-CRIME –includes a wide swath of activities that affect both the individual citizen directly (e.g. identity theft) and corporations (e.g. the theft of intellectual property)

CYBER-INSURANCE – an insurance market covering first and third party risk relating to cybersecurity

CYBER-TERRORISM - criminal acts which involve the use of electronic means

CLAIM – the process by which the insured activates a policy

DEDUCTIBLE –the amount of a claim the insurer is responsible for, before the insurance company will start paying its share of costs

EXCLUSION – those risks excluded from an insurance policy

INDEMNITY – the amount - minus the deductible - that the insured would expect to receive from a claim

INSURANCE CARRIER – is the company holding and supporting the insurance policy purchased from it. The company issues and upholds the risk associated with an insurance policy

INSURANCE POLICY – the document defining what risks or perils are insured along with exclusions

INSURED – the party having taken out or likely to acquire or renew an insurance product

LIABILITY –the state of being legally obliged and responsible under the terms of a policy

PREMIUM – the fee paid by the insured to the insurer for assuming the risk

PRIMARY LOSSES – the direct consequences from the realisation of a risk

RISK – a combination of threat, vulnerability and impact

SECONDARY LOSSES – indirect consequences from the realisation of a risk, which might arise because of the diffusion of information about primary losses

SELF-INSURE – reduction in the size of a loss (the insured covering the costs of a loss itself)

SELF-PROTECTION – measures taken by the insured to reduce the probability of a loss

[1] *Cyber-security and Cyber-power: concept, conditions and capabilities for cooperation for action within the EU*, Directorate General for external policies, Policy Department, 2011.

Executive Summary

In its Global Risks Report for 2011, the World Economic Forum (WEF) reported that concerns about cyber-security were one of the top five global risks along-side demographic challenges and weapons of mass destruction (WMD) identified by senior executives and decision-makers.[2] Despite the emergence of policy initiatives or market based attempts to collect data on cyber security[3] - it would appear that there is still uncertainty as to whether a mature market for cyber-insurance has arrived.

Traditional coverage policies may not comprehensively address the risks faced by an organisation as part of the digital economy. In the UK, only a handful of insurers offer specialist cyber-insurance products, compared to 30-40 carriers in the United States (suggesting that a more mature market exists in the United States).[4] The peculiarities of a cyber-incident, such as its location, severity and visibility, affect the related insurance market, raising different concerns.

In light of this, ENISA conducted a study identifying possible causes inhibiting the cyber-insurance market and investigating incentives to kick –start its development.

The main obstacles identified from the academic literature within the cyber insurance market are:

- ✓ Not enough robust actuarial data[5.] Uncertainty as regard the extent of risk and magnitude of potential losses.
- ✓ Uncertainty about what risk is being insured. Is the prospective insured, for example, looking to cover losses from cybercrime or cyberterrorism? This may result in market fragmentation, especially where theft or general or professional indemnity insurance might already cover general 'cyber-security risks'[6] and given the variety and heterogeneity of risks to be insured (technical failures and disruptions, loss of data and cyber-attacks);
- ✓ Technology drives fluctuations in risk and threats so that it is difficult (from an actuarial perspective) to predict future losses from past events;
- ✓ Lack of upper bound on losses and lack of government intervention as 'insurer of last resort' (e.g. to insure catastrophic risks) may be inhibiting supply of cyber-insurance;

---

[2] *World Economic Forum, 2011.*

[3] *For example, sources of data might include reports from breach notification regime set up under the 2009 EU Telecoms Regulatory Package Art 13a provision for electronic communication service providers to report incidents or the increasing number of data breach surveys published by NIS firms such as Symantec and McAfee or even independent third parties like www.databreaches.org*

[4] *Strategic Risk, March 2012.*

[5] *Although media reports of losses are prominent, there are discrepancies between estimates of losses from a range of sources.*

[6] *This is particularly the case with the difference between primary and secondary losses.*

- ✓ Visibility in the insurance market of the efficacy of various types of cyber-security measures (including whether the demand side considers that existing general insurance is sufficient to cover these kind of risks);
- ✓ Perception that existing insurance products are sufficient to cover cyber-risks.

In addition, there are other characteristics of information markets, well documented in the academic literature, that also are contextually important. These include moral hazard and adverse selection. It is difficult to determine whether they represent cause or effect but they certainly can be seen in the domain of cyber-insurance. Moral hazard deals with the insured's lack of incentives to take initiatives to reduce the probability of loss after having purchases an insurance coverage. On the other hand, in pricing the premium it's essential to identify the likelihood of a potential loss but the existing information asymmetry (private information not available to the insurance company at the time of contracting) affects the insurer's incapacity to differentiate the different types of customer before a contract is signed and therefore price the premium accordingly (adverse selection).

Finally, there is the question of the lack of adequate re-insurance. Re-insurance could act to help reduce the insurers own risk of ruin from a number of claims for large amounts being made at the same time. Its absence might act as a deterrent on the demand side too. This is because the prospective insured might not think the insurer would be able to pay up in the event of a large claim being made and therefore be more reluctant to buy insurance.

Although the theoretical barriers have been documented[7] and explored with a view to finding hypothetical solutions, there is a lack of strong independent empirical evidence as to the strength and maturity of the market.

Moreover, secondary losses deriving from the diffusion of information about primary losses may have counter-productive consequences on the demand side of the insurance market. In other words, those interested in or having purchased or renewing an insurance police might mainly focus on measures to avoid the negative losses from the consequences of a breach (loss in reputation, bad publicity etc…) rather than the cause (poor security practices) in the first instance.

Some possible incentives for the cyber–insurance market are also highlighted, including a set of recommendations for good practices for stakeholders that need to be familiar with this topic. This report does not claim to offer novel solutions to those concerns already identified, rather we try to analyse some of the academic reasoning already articulated in the literature together with the current actual development of the cyber insurance market.

[7] *See Appendix A for an overview.*

We propose four initial domains of possible areas to explore by way of recommendations and we identify the relevant target audience that could support and further explore and analyse their implementation:

- ✓ Collect empirical evidence on the use of cyber-insurance products in Europe, including the types of products purchased, types of risk insured, premiums, payouts etc. in order to thoroughly determine the current and future market trends in this domain. Progressing this recommendation might be included in the efforts of underwriters, firms/organisations and data breach competent Authorities;
- ✓ Explore scope for collective action or redress in order to provide an incentive for firms to take measures to mitigate the financial risks of their cyber-security programs, possible liability arising from class action law suits, in combination with breach notification laws, might have spill over effects in improving the personal data aspects of firms use of cyber-space. Initial fact finding within the European Commission would be a preparatory step to understanding the current landscape in this regard;
- ✓ Consider frameworks to help firms appraise the value of their information, based on information resource management (IRM) approaches so firms can measure the value of information in their enterprise. This recommendation could be further explored by privacy and information security advisors, underwriters and the European Commission. ENISA could also provide support and suggestions;
- ✓ Explore the role of government as an insurer of last resort, building upon other models where policy intervention is in evidence with respect to catastrophic risk. This recommendation could be investigated by Member States and the European Commission.

Introduction

Cyber-security is an increasingly important concern for policy makers, businesses and citizens alike. In many countries, societies have come to rely upon cyberspace to do business, consume products and services or exchange information with others online. In a majority of OECD countries[8], for the period 2000-2009, ICT investments were more important for growth than non-ICT investments. Organisations, both public and private, are reliant upon cyberspace both for driving efficiencies in existing markets (e.g. e-commerce) but for also doing business in-cyberspace. According to Eurostat, nearly three quarters (73%) of European households have Internet access at home and in 2010 over third of EU citizens (36%) bank online.

However, the possibilities for economic and social growth and empowerment are beset by risks, including data and information theft, denial of service and network intrusion. Many of these stem from poor information security practices.

The implications of these risks vary but include possible reputational damage, regulatory exposure (e.g. fines), loss of business and industrial secrets, increased costs of doing business and so on. Latterly, it would appear that many cyber-risks are financially driven and focus on stealing either personal data (given how personal information is now seen as the 'new oil' of the Internet economy) or trade secrets and Intellectual Property theft such as Operation Aurora.[9]

There have been notable examples of both lack of cyber-security measures (vulnerabilities or poor security practices) and further impacts. Examples include the loss of some 25m records by the UK Inland Revenue and the recent data breach from Sony Online where 24m customer records were stolen.[10]

Consequently, cyber-insurance has 'captured the imagination' of many involved in cyber-security at the policy and research level, as a mean to transfer these financial risks to third parties.[11] One of the interesting aspects is that even a cursory informal search of publicly available data brings up limited information on the size of the cyber-insurance market in Europe. Further afield, in 2011, the Betterley Report[12] concluded that the US cyber risk market the estimate of the total written premiums (not assets insured) was US$800million[13].

In the US and UK we identified some evidence of insurance carriers offering products ranging from cyber-liability to network outage products. In the UK for example, well known insurers such as Chubb and Zurich are known to offer products. In the US more recently, Chartis has launched a 'catastrophic risk' insurance product offering coverage up to US$100m.

Things that appear to be driving the market are privacy (perhaps spurred on by data breach notification measures) and the alleviation of post breach costs (remediation) and reputational

---

[8] *The OECD includes 34 member countries, from North and South America to Europe and the Asia-Pacific region.*
[9] *The Security Blog, 2011.*
[10] *The Guardian, 2011.*
[11] *(Böhme and Schwartz, 2010).*
[12] *Betterley, 2011.*
[13] *Exchange rate as of 5th June 2012: 1 euro = 1.2429 USD.*

risk. These may include fines, penalties, damages, settlements, and legal costs from either a data subject or regulatory body.

Policy context

At the European level, the 2006 Strategy for a Secure Information Society- Dialogue Partnership and Empowerment explicitly identified market based incentives as a way to improve levels of cyber-security[14] and avoid possible market intervention.[15]

The establishment of the EU Telecom Package Article 13a breach notification regime is one plank in the evolving European regulatory regime governing cyber-security which will lead to a more systematic collection of actual data in relation to incidents. The EU Directive 2009/140/EC[16] amends existing directives on telecommunications networks and associated facilities. Article 13a introduces a requirement for providers of public communications networks to take measures to guarantee the security and integrity of these networks and to ensure continuity of services provided over these networks. In particular, paragraph 3 says that providers should report significant security breaches and losses of integrity to the respective National Regulatory Authorities (NRAs). Annually, summary reports should be sent to ENISA (European Network and Information Security Agency) and the European Commission. The aggregated analysis of the incident reports will describe the current trends[17] and provide knowledge and information to NRAs and operators.

Similarly, the recent announcements under the reform of the EU's legal framework governing privacy and data protection that breach disclosure reporting (with possible fines) has the potential to play into the market communication of risk. In January 2012, EU's Justice and Fundamental Rights Directorate General disclosed that breach notification was being proposed to apply to certain Internet businesses controlling or processing personal data (in line with the extant EU Data Protection Directive 95/46/EC). The proposed law would require such business to inform a regulator within 24 hours after having become aware of an attack and data subjects as soon as reasonably feasible.[18]

The current regime for notification of breaches of personal data envisaged in the revised Directive may lead firms to focus on secondary losses (investing in management of the reputational fall out from a loss of personal data) rather than primary losses (the direct & immediate costs of the loss). Indeed, the short time limits proposed may further incentivise the affected firm to consider secondary rather than primary losses. It may thus be seen that

---

[14] *Notwithstanding the possibilities for the insured to indulge in more risky behaviour after a contract is signed.*

[15] *COM (2006) 251, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, A strategy for a Secure Information Society – "Dialogue, partnership and empowerment".*

[16] *Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services*

[17] *The trends will refer to the incident root causes and the actions taken.*

[18] *CIO.com, 2012.*

like many other areas of regulatory intervention, it addresses the symptoms and not the cause of cyber-security problems. One might further observe that a flourishing market will develop not aimed at remediation of the vulnerability that causes the loss but rather 'reputational management' for firms to reduce (if they can choose to disclose) secondary losses. This may lead one to draw the conclusion that what is currently labelled as cyber-insurance is not for cyber-attacks, but instead for secondary losses (e.g. reputational damage).

Since there are different views in the literature about whether being insured is the IT risk or the cost of IT risk (conceptually two different things) perhaps better information on the likely costs of IT risks would help to address these problems. Note that this is different from a breaching cost, which takes into account and may perhaps even focus exclusively on secondary costs.

Whilst the creation of a breach notification regime may be considered a useful contribution to the market for cyber-insurance by reducing information asymmetries, its effectiveness could be undermined without regulatory intervention to stimulate other attendant aspects. This includes:

- ✓ Making it easier for private legal cases to be launched (e.g. via considering opportunities to adjust the regulatory regime to permit class action cases in this domain in Europe);
- ✓ Robust, pan European valuation of the costs of IT breaches (via collection of data across a broad range of firms);
- ✓ Mandatory insurance for certain areas (perhaps using public sector procurement as an initial stimulus – to be eligible to bid for a public contract, a firm must possess appropriate insurance coverage).

Finally, an example of recent relevant regulatory intervention from across the Atlantic can be seen in the United States where the Securities and Exchange Commission (SEC) in 2011 required that all regulated firms should disclose the risk of cyber incidents. Expectations in the market are that this will trigger many firms buying cyber-insurance in order to communicate to the market information that they are properly managing these risks. The new rules also require those regulated by the SEC to evaluate and take into account all available relevant information including prior cybersecurity incidents and severity and frequency of those incidents. Disclosures under these rules require that the regulated firms include a description of relevant insurance coverage.[19]

Objectives of the Study

This scoping study summarises the evidence identifying barriers to cyber insurance (interdependency of assets in cyberspace, correlated risk and information asymmetry) and empirical insights derived from desk research, knowledge of the study team and input from an Expert Review Group. This is in an attempt to answer the question as to whether the

[19] *U.S. Securities and Exchange Commission, CF Disclosure Guidance: Topic No. 2, Cybersecurity (October 13, 2011).*

continued absence of a robust and flourishing market is down to the 'mere' absence of data or whether there are more systematic concerns at hand. The Study proposes some possible incentives for the development of the cyber- insurance market and provides the readers with a set of recommendations for those facing the issues related to the Study.

Target audience

The main audience for this report is policy makers or generalists who are required to be familiar with the broad implications of these issues.

What is cyber-insurance?

Cyber insurance refers to insurance contracts having the purpose of covering a broad range of issues relating to risks in cyberspace. Researchers have identified contracts as covering things like: liability issues, property loss and theft, data damage, loss of income from network outage and computer failures or web-site defacement.[20] Other examples may include data asset protection, cyber-extortion and, more indirectly, liability arising from negligence relating to personally identifiable data. In addition, there is also coverage for cyber-liability which covers the insured's liabilities (defence and compensatory damages) where a third party, under a negligence claim, can pursue a tortuous or delict[21] claim for injury. For example: the third party being affected by a virus; personally identifiable data belonging to the third party was disclosed or the business of the third party was interrupted as a result of negligence by the insured. For example, the stand alone policy form offered by the Insurance Services Office[22] includes coverage in the following areas:

- ✓ Security breach liability and expense;
- ✓ Programming errors and omissions liability;
- ✓ Replacement / restoration of electronic data;
- ✓ Business interruption losses and extra expense;
- ✓ Public relations expense;
- ✓ Website publishing liability.

Many first and third party risks of this nature are generally excluded from traditional commercial general liability policies.[23] An insurance contract (policy) binds an insurance company in the occurrence of contractually defined loss events to pay a specified amount (claim) to the insurance holder. In return, the insurance holder pays a fixed sum (premium) to the insurance company.[24] The cyber-insurance contract is signed between the insured company and the insurer and includes aspects relating to the selection of the coverage type, the risk assessment phase of security and cyber protections and the evaluation of the security systems and tools by IT specialist and insurer. Based on the assessment and value of this information, the amount of the premium is then calculated[25].

[20] *(Bandyopadhyay 2009).*
[21] *For the purposes of this report, delict may be thought of as the broad equivalent of tortuous liability in civil law based countries.*
[22] *Insurance Services Office, 2009.*
[23] *Cyber –Insurance Metrics and Impact on Cyber –Security available at www.whitehouse.gov.*
[24] *(Böhme 2005).*
[25] *(Ghavami, Kalantari, Rahimi, 2009).*

The basic characteristics of insurance

The basic indemnity insurance model, proposes that risks that can be insured possess seven common characteristics[26]:

- ✓ Large number of similar exposure units (the more data points the more likely that predicted losses become similar to actual losses);
- ✓ Definite loss –the loss takes place at a known time, in a known place and from a known cause;
- ✓ Accidental loss – the event leading to the loss is not something that the insured has any discretion or control over;
- ✓ Large loss –the size of the loss must be meaningful from the perspective of the insured;
- ✓ Affordable premium – the premium offered must be proportionate to the amount of protection offered, otherwise the prospective insurer will simply self-insure;
- ✓ Calculable loss – both the probability and the attendant costs must be estimable if not calculable;
- ✓ Limited risk of catastrophically large losses – if the losses are independent and non-catastrophic they are not likely to bankrupt the insurer.

The case for cyber-risk as an insurable form of risk

In many respects, cyber-security risks appear to exhibit some of these properties as to make them a valid candidate for insurance. Many people use similar operating systems, software (e.g. web-browsers) so there are a large number of similar exposure units. Moreover, there is the potential for accidental loss.[27] Premiums can be affordable (although this is linked to some of the issues discussed in this report, that the premiums may be too high because of a lack of demand) compared to the costs of implementing expensive cyber-security measures; there are calculable losses (certainly the attendant costs for first party liability can be estimated and for some cases it is possible to estimate probabilities).

Finally, it is certainly possible to identify the time of a loss (but perhaps not as clearly its location or cause). Conversely (as we shall see) losses might be interdependent (correlated) and there is uncertainty as to the upper bound – there is no robust data which would help underwriters predict, calculate losses or indeed whether they might be catastrophically large.

Other rare or specialised risks

It is also worth considering some other markets where there are rare risks that nonetheless get insured without actuarial tables. Insurance in these areas seems to exist contrary to the common characteristics of insurable risks identified above. We list some examples of insurance for other rare risks below:

---

[26] *(Mehr and Cammack, 1980).*

[27] *The complexities of attribution mean than determining whether something is accidental is not trivial.*

- ✓ Offshore oilrigs are a first interesting case in point. In this case, companies offer different types of insurance to cover property (physical damage), windstorm, non-gradual pollution, control of well, terrorism, construction and cargo.[28] Insurance in this area is closely related to pollution insurance that covers the social and environmental consequences of events like the Deepwater Horizon incident;[29]
- ✓ Satellite insurance is also a case in point that has the properties of being complex and beset by rare risks.[30] Satellite insurance may cover three main types of risk: re-launching the satellite due to failure of the launch operation; replacement of the satellite if it is destroyed, placed in an improper orbit or fails and finally liability for damage to third parties cause by the satellite or launch vehicle. Due to the military implications, the information provided to insurers is very limited since the information could be used for missile technology purposes. The satellite insurance market also has a secondary reinsurance market;[31]
- ✓ Finally, as a non-technical example, coverage for industrial disputes may also offer some useful comparisons.[32] Insurance for industrial disputes is now much wider and covers more general business interruption including interruption resulting from industrial action.

The evolution of specialised insurance markets

Specialised insurance markets may to a certain extent be characterised by a quality of circular logic, namely would firms be as willing to invest in oil rigs or satellite launches without insurance. It is worthwhile to consider some illustrative aspects of this and how specialised markets evolve. We do this in order to provide illustration of how analysis of the evolution of a market for specialised risks might apply in the case of cyber insurance.

In the example of satellite insurance, when the commercial potential of satellites emerged after the mid-1960's it became clear that a market for insurance was available. The American Communication Satellite Corporation (ACSA) led demand for satellite insurance. Early examples of satellite suffered due to unreliability of vehicles and the experimental nature of payloads, so governments retained the risk. Although insuring satellite risk was a practice within the aviation industry the complexity of insurer knowledge required for pricing and claims handling led to a specialised market. There are a limited number of insurers offering satellite coverage although the market is global in nature. The satellite insurance market is also interesting in that the number of launches is less than what is expected to be a minimum threshold for determining risk. In addition, the early stages of the market suffered from generic losses (breakdowns recurrent in similar satellite's platforms). Generic defects are excluded at policy renewal.

---

[28] *(Mankabady, 1985).*
[29] *(Force, Davies and Force, 2011).*
[30] *(Weiss and Manikowski, 2007).*
[31] *(Fordyce, 1985).*
[32] *(Foster, 1971).*

Finally, there is also indication of how insurance markets may go through underwriting cycles which is defined as an alternating periods of hard markets when insurance prices and profitability are high and soft markets when insurance prices and profitability is low.[33] However, such considerations have difficulty in distinguishing between price per exposure or breadth of coverage in driving such cycles.

Understanding models for cyber-insurance

Existing economic models for portraying the cyber insurance market differ in relation to demand and supply sides respectively referring to the insurance carrier holding and supporting the insurance policy (supply) and firms considering taking out or renewing insurance products (demand). Researchers have also considered other elements including:

- ✓ the network structure (encompassing defence functions, network topology, risk arrival and attacker model);
- ✓ player information (e.g. informed or uninformed);
- ✓ actions of the players;
- ✓ timing of these actions.[34]

Early literature discussed two main reasons for the lack of a market – the low levels of familiarity with this new type of risk and poor actuarial data. Further efforts by economists tried to broaden understanding of possible barriers. Subsequently, understanding of the demand side of the cyber-insurance market seeks to explain market failure based on the lack of equilibrium.

Commonly, theoretical analysis usually portrays this in the context of the following three properties of cyber-risk:

- ✓ Interdependent security – the risks faced by a firm depends not only on its own choices but also on those of others. As more firms decide not to invest in security, the probability of a successful terrorist attack grows, and there is no economic incentive for any specific firm to invest in security. As the number of firms/organisations gets large, a firm will not be willing to incur any costs to invest in security because it knows it will be contaminated by other unprotected firms[35];
- ✓ Correlated risk – a supply side problem where the many potential losses from a single event can be so extensive as to force insurers not only to price contracts to accommodate these losses but also to protect against the possibility of themselves suffering ruin by multiple claims occurring at once. This is seen by some as being

[33] *(Cummins and Outreville, 1987).*
[34] *A unifying framework to understand cyber-insurance has been proposed in the literature (Böhme and Schwartz, 2010) see Appendix A.*
[35] *Kunrether and Heal, 2003 and Geoffrey Heal, Michael Kearns, Paul Kleindorfer,and Howard Kunreuther, 2006.*

driven from monocultures of equipment (a single vulnerability affecting many) and therefore an opportunity for market intervention[36];

- ✓ Information asymmetries – specifically insurers lacking information on the risks that the insured may be bearing which can also lead to adverse selection (where the insurer cannot efficiently segment the market, leading to insurers inefficiently pricing premiums on the basis of the 'lowest common denominator'). This is compounded by the aspect of network externalities as a common characteristic of cyberspace related phenomena. The related aspect of moral hazard (where the insured may act in a more insecure manner by investing in less security after the acquisition of insurance because they now know that the insurer will bear some of the negative consequences) informs this consideration.[37] In either case these situations reflect opportunistic behaviour on the part of either the supply or demand side of the market.

[36] *(Böhme and Kataria, 2006).*
[37] *e.g. see (Bandyopadhyay, 2009) and (Pal, 2012).*

Why cyber-insure?

Some of the measures that can be taken by a firm to protect itself against damages arising from a cyber-incident can be identified as: self -protection, self-insurance and cyber-insurance. Self –insurance and cyber-insurance both aim at the reduction of the losses' size. With cyber insurance the firm purchases insurance from a third party while self-insurance is an internal investment to be used in case of loss. On the other hand, self-protection attempts to reduce the probability of any losses that may occur.[38] In addition, a firm may be exempt from liability in certain regulated areas as stipulated by criteria set out a specific National Regulatory Authority.

Given the high transaction costs associated with liability rules, implemented through the court system, and safety standards imposed by regulation, cyber-insurance may offer a good option for transferring risks that can be transferred. Furthermore, cyber-insurance could prove to be attractive in transferring financial risk particularly with respect to third party risk, costs of legal action (defence and compensatory damages) and regulatory fines.

[38] *(Kesan, Majuca,Yurcik 2004).*

Current Market Offerings

Confounding the theoretical barriers and literature indicating that there is no mature cyber-insurance market identified above, according to a recent report by Lloyds, the market for cyber-insurance has 'taken off'.[39] This is spurred on by strengthened legislation in both the US and Europe. Sectors typically buying cyber insurance include retailers, healthcare providers, hotels and financial services – all of which typically buy data breach insurance. Demand was reported to be growing amongst UK and European companies following expectation about regulatory intervention for breach notifications. The state of market offerings is also of course related to the question of re-insurance with which we deal below. Nonetheless, some industry data as presented appears to contradict the assertions that this market is either immature or non-existent.[40] At a recent conference on emerging risks, it was suggested that the overall UK market (in terms of exposure for claims) for cyber-insurance was worth US$250m.[41]

Evidence from the industry[42] suggests that insureds currently are covered (or think they are) for cyber-risk under:

- ✓ Commercial General Liability (CGL) or a modified CGL policy which includes (endorses) cyber-risk;
- ✓ Misused other policies (e.g. business interruption);
- ✓ Standalone cyber-policies.

Evidence from a UK based industry representative suggests that the current size of the market (in terms of gross written premiums (according to those filed under relevant Lloyds codes) is £3-4m. Globally, the estimates range from US$500m-US$700m.[43] In the last 10 years, the market has evolved considerably, driven by notification laws in the US. In Europe, however, it was observed that there was slower growth due perhaps in part to the differing legal framework. Up until now in the UK, it was seen that cyber-insurance was a rare product and seen as incidental and often added to Commercial General Liability (CGL), E&O (Executives and Officers) liability or business interruption.[44]

Types of insurance product known to be offered include coverage for human error, program error, system outage and Distributed Denial of Service (DDoS).

The market is being driven by first party notification which is also resulting in spill over effects into non-tangible business interruption. The market is expected to substantially evolve, driven by insured looking either initially at first or third party coverage.

---

[39] *(Lloyds, 2011).*
[40] *For example, five companies have been identified as offering products in this domain: Barbican, Chubb, Hartford, LIU and Zurich.*
[41] *Perrin Conferences, 2012.*
[42] *(Attansani, 2012).*
[43] *Gareth Tungatt, personal communication 23rd April 2012.*
[44] *It is understood that in 2013, Lloyds of London will add a new business class code (category) covering cyber-insurance.*

Other specific concerns reported from the industry[45] relate to the question of how to measure intangible information (covered below in the section on information asymmetry) and whether organisations that had taken out CGL policies were in effect 'misusing them' by expecting that they would be covered for cyber-risks.

The question of how to value intangible assets in particular comes into play with standard business interruption insurance policies, where the tangible loss has to be demonstrated. This is defined as the hardware (laptop, USB stick etc) rather than the (potentially more) valuable information stored upon such devices.

In the US a number of court cases have explored and tested this distinction. These mostly cover claims made by policy-holders under CGL policies and there is no significant body of decisions (in the US) regarding stand-alone cyber-insurance policies. There are reportedly no examples of similar cases across the EU. Attisani identifies some relevant cases often cited by the industry which include:

- ✓ Whether damage to a third party's computer software or data constituted property damage (cases of American Guaranty & Liab. Ins. Co. v Ingram Micro Inc, 2000 and America Online Inc v St. Paul Mercury 2003);
- ✓ Insurers then began to amend their CGL policies to explicitly indicate they did not cover customer's loss of data (case of Eyeblaster Inc. v Federal Ins. Co. 2010) allegedly caused by spyware from the insured – endorsements subsequently offered by insurance carriers that add 'third party's computer data and software' as things that are covered – but not firms own electronic data;
- ✓ Cyber-crime (case of Vonage Holdings Corp. v Hartford Fire Ins. Co (2012) where the insurance carrier argued to dismiss claims relating to a computer fraud section of a crime policy after a criminal accessed Vonage's own computer network and hijacked servers.

Supply side

The insurance carrier issues and upholds the risk associated with an insurance policy. The 2011 Betterley Report concluded – based on a survey of the cyber/privacy/media liability market in the US - that there were some carriers in the market but that the number of data breaches is increasing, raising a note of concern as to whether coverage will remain available concludes. This report also defines insurance products as covering data risks for example losses of customer client records, e-commerce (selling products, services or content) or social networking. It goes on to remark that, in 2011, premiums increased and carriers were reporting a large amount of business.[46] In the UK, only nine insurers have specialist cyber-insurance offerings, compared to 30-40 in the USA (suggesting that a more mature market exists).[47]

[45] *Perrin Conferences, 2012.*
[46] *(Betterley, 2011).*
[47] *Strategic Risk, March 2012.*

In December 2011, Chubb, an insurance company, reported that it launched a new cyber-insurance product for companies in the UK, Ireland and Europe that owns or controls confidential, sensitive, financial or private healthcare data.[48]

Demand side

The demand side is made up of organisations interested in or having purchased or renewing an insurance policy which covers them in case of a realisation of a risk. PwC's Global State of Information Security Survey in 2010 reported that 4 out of 10 firms surveyed were taking out insurance policies to protect against damage caused by data loss.[49] This is driven by high profile legal problems, according to the firm.

According to a 2011 survey[50] one third of organisations reported as having purchased cyber liability insurance as part of a cyber-risk management strategy.[51] Comments provided as to why companies might not purchase include:

- ✓ Investment in prevention rather than insurance;
- ✓ Limited markets;
- ✓ Broker disconnects (problems between the broker, carrier and insured);
- ✓ Lack of coverage clarity;
- ✓ Lack of information to make informed decisions;
- ✓ Too expensive;
- ✓ Application process is difficult;
- ✓ Deductibles are too high;
- ✓ Difficult to quantify;
- ✓ Policy coverage is too limited.

Nearly half of respondents not currently buying such insurance are either not sure or are considering buying such insurance, a finding reported as representing a growth opportunity for brokers and insurers.

The Insurance Information Institute[52] reports that limited coverage under traditional policies is beginning to be available. Policy holders look to traditional business insurance of different types to cover emergent cyber-risks:

- ✓ Property insurance (including business interruption coverage);
- ✓ Liability insurance (including Errors and Omissions (E&O), Directors and Officers (D&O), general liability and umbrella insurance);
- ✓ Crime insurance policies (including financial institution bonds, computer crime policies and fidelity insurance);

[48] *(Chubb, 2011).*
[49] *(PwC, 2010).*
[50] *Survey sponsored by Zurich .*
[51] *(Advisen, 2011).*
[52] *The US based insurance Information Institute is an association representing the insurance industry.*

- ✓ Business owners' policy (BOP).

The focus on first party cyber risk appears to be low in comparison to third party risk. First party risk may cover aforementioned direct losses such as business interruption and loss of digital assets. By comparison third party liability cover appears to becoming popular (driven by the increasing enthusiasm for breach notification laws in both Europe and the United States). Third party liability covers liabilities in the event of a data breach (of various types).

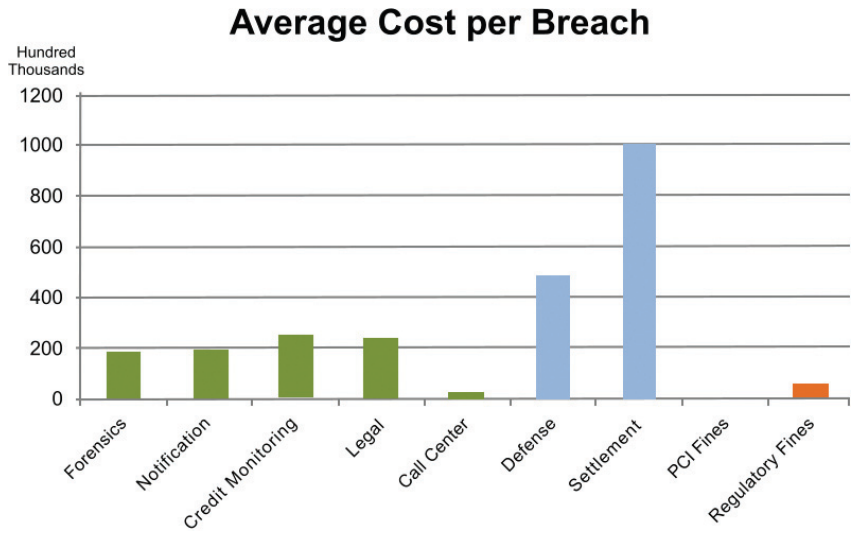
Market data from actual claims

In 2011, a US market study on empirical evidence from covered events and actual claims pay-outs presented data from major underwriters of cyber liability pay-out information based on 117 incidents between 2005 and 2010.[53] This found that personally identifying information (PII – personal data in the EU context) and personal healthcare information (PHI) were the most exposed data type.

The average cost per breach based on data from underwriters was US$2.4m excluding an outlier of a billion dollar business interruption event. The average cost per record was US$1.36 whereas when outlier events involving millions of records were excluded the average cost per breach was US$5.00. Interestingly, legal damages represented the average largest component of costs, with the average cost for legal defence being US$500,000 and the average settlement costs of US$1m[54]. This finding seems to support an argument that insurance is aimed at liability claims and not primary direct losses.

[53] *(Greisiger, 2011).*
[54] *Exchange rate as of 5th June 2012: 1 Euro = 1.2429 USD.*

Figure 1 below indicates the segmentation of costs per breach for the United States.



Source: Cyber Liability and Data Breach Insurance Claims: a Study of Actual Pay-outs for Covered Data Breaches (2011)

Cyber-insurance market barriers

Insurers commonly purchase reinsurance to protect themselves against extreme losses. The limited nature of claims experience relating to cyber- security and the lack of definitive figures of costs associated with different risks and security failures makes it difficult for the insurance and reinsurance industries to grow. In this section we detail a number of reported obstacles as to why the cyber-insurance market still has not yet taken off.

The lack of solid data on losses has been claimed to be one of the key concerns about cyber-insurance. It contributes to the problem of information asymmetry between both the insured and the insurer. For the insured, there is the question of understanding the competitive pricing of products if they themselves have little or no appreciation of the likely primary (direct) or secondary (indirect) losses. For the insurer, there is the question alluded to by researchers about the ability to accurately price contracts.[55]

Another important concern is the definition of what risk is being insured. The rapid change in technological landscape may result in 'ambiguity and misunderstanding' about what risks are being insured[56] also given their high variety and heterogeneity (e.g. technical disruptions, loss of data, exfiltration of proprietary information and so on). The use of best practice and technology neutral security standards might help alleviate such concerns.

The lack of adequate reinsurance is the third barrier identified. The lack of robust actuarial data impedes a precise estimate of actual damages that could arise from cyber-incidents. This poses concerns not only to the insurance companies but also to reinsurance ones consequently restricting their development.

Uncertainty about the extent of risk and lack of robust actuarial data

The lack of solid actuarial data often feeds into two problems about cyber-insurance. Firstly, the question of adverse selection (the insurer cannot differentiate different types of customer before a contract is signed and therefore price the premium accordingly) and, secondly, the moral hazard where the insured, once a contract is signed, may be incentivised to behave more insecurely in the knowledge that the insurer will bear some of the loss.[57]

This paucity of robust evidence of cyber incidents/attacks is often cited as one of the reasons for the poor or hobbled cyber-insurance market. This is despite an increasing flood of information concerning information about cyber-attacks and the costs and implications of such incidents.

---

[55] *(Bandyopadhyay, 2009).*

[56] *Baer, 2003. Baer cites the Ingram case in the United States about the difficulty of interpreting what constitutes physical damage.*

[57] *It is also possible (although as yet untested from a theoretical or empirical perspective) that behavioural conditions (e.g. how individuals make decisions on behalf of their organisation, and the collective decision-making culture of the prospective insurer) also play into the question of moral hazard: however, this is also the case with other cyber-security related issues.*

Sources providing this include:

- ✓ Surveys such as the US Computer Security Institute/Federal Bureau of Investigation survey, the UK's Information Security Breaches Survey; the BSI's survey;
- ✓ Criminal Justice statistics which cover cyber-crimes but are beset by the usual concerns of criminal justice statistics (namely under-reporting, normalisation and double counting) – examples include the European Sourcebook on Criminal Justice Statistics which covers recorded cybercrimes;
- ✓ Reported figures from for profit companies such as Norton's 2011 Global Cybercrime Survey or the Ponemon 'cost of cybercrime breach' survey (where the provider may be incentivised to firstly over-estimate the figures to demonstrate the need for a market and also show that the problem is getting worse);
- ✓ Independent quantitative data such as surveys, real-time data and research such as metrics provided by small non for profit research organisations like datalossdb.org or Team Cymru;
- ✓ Data from Computer Emergency Response Teams (CERTS) which may also be subject to considerations about reliability and the gap between real incidents and incidents where the affected party can report.

Despite this flood of information, decision-makers are confronted with uncertainty about which to believe and whether one should be relied upon more than another.

Finally, it might be argued that this barrier affects both sides of the market, rather than others which may lead to moral hazard or adverse selection, causing opportunistic behaviour in either supply or demand.

Uncertainty about what risk is being insured

The rise of personal data and the increasing use of social media are confounding and complicating consideration of risks. This may be seen to be a shift in focus away from insuring the costs of reconstituting IT systems identified in the theoretical literature[58] toward liability issues associated with privacy, intellectual property and employment practices.[59] Liability issues include regulatory intervention (e.g. fines from privacy regulators) and various types of civil litigation including defamation and tortuous claims. This may be seen as an expansion in the breadth of risks to be covered.

In particular, this is reflected in relation to primary and secondary losses. Since the secondary losses (reputational ones) may differ between prospective firms (publicly or non-publicly listed), insurers might be confronted by uncertainty about what risks they can insure.

[58] *(Böhme and Schwartz, 2010).*
[59] *(Hartwig and Wilkinson, 2011).*

There is also the question about policy exclusions that may not cover claims resulting from certain types of risk such as state sponsored cyber-attacks.[60] Some researchers have attempted to separate out systemic risks (which may occur to anyone) to symptomatic risks (which are down to the specific poor security levels in the prospective firm).

Based on the model of systematic and symptomatic risks, it may be argued that such risks are systemic[61] and are thus precisely those types of risk where no amount of investment in cyber-security by the firm would be sufficient.[62] The question of determining attribution for cyber-attacks is of current interest in the debate if and how it is necessary to resolve the inherent trustworthiness of cyberspace. Although some intelligence agencies and national security organisations claim that attribution is possible, the (admittedly wide) gap remains between those possessing this knowledge and the insurance market that could use this to better determine where risks and perils are the result of *force majeure*, *acts of God* etc..

Technological evolution

The fast-paced nature of the use of technology has implications for the insurance market in terms of being able to keep up with technology presents new vulnerabilities and new avenues for threats to manifest themselves. As current examples, mobile phone operating systems are becoming attractive targets due to the increasing use of these devices and the relatively low level of attention given to security by some operators.[63] To use the standard understanding of risk in this field, this may include the three dynamics of:

- ✓ Threat –in the criminal case, the rise of the 'post organised' underground criminal economy, which would appear to be based on a service-led model and currently takes advantage of the technical platform of botnets as a broad means for the perpetration of a wide variety of cyber-attacks and cybercrimes;
- ✓ Vulnerability – at the structural level (e.g. the DNS or Inter-domain routing), within organisations (e.g. deployment of poorly secured technologies, lax security processes) but also technological (poorly designed and secured software code);
- ✓ Impact – the prospective insured likely losses as a result of the use of technology. This is related to the ability of the insured to value intangible assets like information.

Little visibility on what constitutes effective measures

There has been a range of measures and efforts to identify what constitutes 'good' cyber-security. These include the promulgation of best practice such as adherence to the ISO 2700x suite of security management standards. If a company can show that it has adopted a set of practices generally considered by the community to be worthwhile things to do with respect

---

[60] *The question of when a state sponsored cyber-attack may be attributed as such is not just vexing for the national security community but also in the domain of cyber-insurance. If policies exist that specify the government as 'insurer of last resort' then a system of alerting insured firms, under such a scheme, that a specific cyber-attack was 'state sponsored', thereby invoking the government to foot the bill for losses, would need to be established.*

[61] *They are not symptomatic of the relative level of cyber-security of the insured but rather affect all with an equal probability.*

[62] *(Bandyopadhyay, 2009).*

[63] *(Georgia Tech, 2012).*

to cyber-security, then this will reduce information asymmetries and better demonstrate to the market that the firm takes security seriously. This feeds into premiums so that if an insurer can observe that a firm is undertaking various 'effective' security measures, then the premium will be reduced on the basis that the prospective firm is less prone to risks.

As an example, in 2012, the industry based Cyber-Insurance Working Group was announced. [64] This is being run by NCC Group, an independent information security firm and is reported to consist of firms like Zurich Insurance, Liberty International Underwriters (LIU) and CNA Europe. The objective of the Working Group is to develop on recommended information security practices and policies including business continuity planning.

The parlance of risk management has become into common usage concerning cyber-security. Some of the earliest investigations into cyber-insurance recognised the need to identify and quantify potential losses and the uncertainties surrounding them.[65] This enables IT security professionals to more objectively consider how much to invest in resources and whether they will be effective in mitigating against a particular type of risk.

The exploration of what constitutes effective security has led to identify a range of different approaches to understanding the cost benefit analysis of one measure over another.[66] These include: macro-economic input /output models evaluating the sensitivity of national economies to cyber-attack in particular sectors; econometric techniques; return on security investment analysis; characterisation of real world decision-making; heuristic models which rank costs, benefits and risks of different strategies; risk management frameworks and methods from game theory. Nonetheless, despite such analysis reporting how firms can understand the relative effectiveness of different measures there remains significant confusion about what constitutes 'good' security.

Similarly, on the other side of the coin, there have been studies showing the effect of incidents on stock market valuations of firms. Although as we have seen care must be taken when analysing such data to tease out the difference of the market 'measuring' the ability of the firm to manage negative PR from breach (thus minimising secondary losses) with the intrinsic (in)security in the first instance.[67]

---

[64] *Insurance Networking News, 2012.*
[65] *(Baer, 2003).*
[66] *(Rue et al., 2007).*
[67] *For example, (Cavusoglu et al., 2004) performed an empirical review of stock market prices of publicly listed firms, finding that disclosed IT security breaches reduce the stock price of a firm. Although this happens over a short term, it would appear from this limited study that the market reacted negatively to news of the breach, possibly indicating the poor levels of IT security within the firm. It must be noted, however, that this might also reflect the firms' poor ability to manage the secondary losses from a breach (i.e. mitigating the bad PR). Nonetheless, this study found that over the course of a few months, the stock price returned to near previous levels. In 2006, (Ko and Dorantes, 2006) conducted an empirical study over four economic quarters which investigated the impact of information security breaches on firms performance, finding that the breached firms sales and operating income did not decrease, return on assets did and the performance of the control (non-breached) group was higher. Interestingly this study found that the sales of the breached firms increased significantly in the fourth quarter of the period under review.*

Nonetheless, there are caveats to the approach of looking at share price as an input (and possible incentive) for the cyber-insurance market. Firstly for the incentive of notification affecting negatively the share price to be effective the firm must be publicly listed (not all firms are) and secondly evidence that the share price, over the long period of time returns to normal. This is compounded by the understandable expected market reaction to a low share price of a firm that perhaps has solid 'fundamentals' but has suffered a breach – that market players see shares in a going concern priced cheaply thus leading them to buy, pushing up the price. Finally, the implication of this is that firms might spend more to try and reduce the risk of news getting out of a breach, rather than actually fixing the levels of insecurity that was the origin of the problem.

There is finally one aspect that perhaps cyber-security is in and of itself un-insurable – in the sense that quantification as a route to informing a market is a dead-end. Quantified security (one of the building blocks of insurance) is, in and of itself, an assertion supported by methods with unclear validity according to some recent thinking.[68] The lack of validation suggests that quantification and the lack of comparison between such models and empirical evidence presents further risks to the use of such models, which may be irrational for an operational decision-maker depending on such methods. The lack of solid data is regarded as a crucial missing element. The inherent uncertainty in security decisions may lead to over confidence in available (but invalidated) quantitative information.

Absence of insurer of last resort to re-insure catastrophic risks

In the re-insurance market the risks of rare catastrophic events may be pooled in a higher order setting thus permitting equilibrium and the presence of a market. Given the extensive losses identified by some security service providers, the question of whether the possibility for unlimited liability is a barrier to cyber-insurance merits further consideration. As a possibly rare example of a product, in April 2012 the US firm Chartis launched its CyberEdge Tower insurance product, a network security 'cat-risk' product aimed at providing coverage of total aggregate limits of liability up to US100m.[69]

The aspects of catastrophic loss can be seen in how Lloyds market suffered from an exceptional number of catastrophes in the 1980s and 1990s. The losses amounted to €16bn over five years resulting in 1500 out of the total 34,000 Lloyds members being declared bankrupt.

The costs from the terrorist attacks of Sept 11th were US$32.5bn according to reported data from the US based Insurance Information Institute. The costs of claims pay-out from Hurricane Katrina were US$41.1bn. Terrorism reinsurance may be regarded as a useful example in understanding how unlimited liability plays out.

In 2010, the OECD discussed various types of catastrophic risk such as natural disasters, terrorism and one best practice alluded to was the use of public private partnerships where

[68] *(Verendel, 2009).*
[69] *Insurance Journal, 2012.*

the state takes a role in being a backstop for the market. This is particularly the case as the state has a responsibility in the prevention and mitigation of terrorist attacks. The summary from the 2010 conference reported that a great many permanent and temporary solutions exist – 9 OECD countries out of the 31 had set up various mechanisms to permit government stakeholders to intervene under pre-determined thresholds and where the government intervenes as a re-insurer of last resort.[70] Whilst noting that current coverage is based on voluntary cover, discussion also took place about the possibility of expanding scope to cover all relevant lines of business affected by a terrorist incident since presently property was generally only covered by programs.

At the national level, in 2002, the US government passed the Terrorism Risk Insurance Act (TRIA) which was intended as a backstop for insurance claims related to acts of terrorism. TRIA creates a US government re-insurance facility to provide coverage to companies following a declared terrorist event.

In the UK, Pool Re was established following the 1993 bombing of London's financial district by the Provisional Irish Republican Army as a way that insurers can continue to cover losses resulting from damage caused by acts of terrorism to commercial property in Great Britain.[71] Insurers are able to draw upon reserves accumulated on a mutual basis within a separate company if they are required to pay losses exceeding a threshold set by the insurer and the insured. Pool Re, the separate re-insurance company is further able to draw upon funds from the government to enable it to meet its obligations in full. At present, Pool Re does not cover damage to computer systems caused by virus, hacking and similar actions. An official confirmation that an act of terrorism has taken place must be agreed by the UK Government, which issues a certificate under an agreed procedure.

However, due to the aforementioned characteristic of the interdependency of risks in cyberspace, the idea of pooled re-insurance is largely seen as unattractive by researchers. The prevalence of a broad installed base of similar systems (monoculture) means that re-insurers would not have independent risk pools.

Perception that existing insurance already covers cyber-risks

A final possible contributing factor is that perhaps firms already think that they are insured under existing more general business interruption policies. This would lead them to be deterred from taking out specific cyber-insurance policies on the basis of a fear of being over-insured. This is compounded by the question of adverse selection since the supply side cannot segment the market efficiently enough. However, identifying this as a barrier is complex because it is necessary to separate out specific products in this field from additional coverage under traditional polices. Nonetheless, this can be explored by reference to the more general business insurance market.

[70] *(Organisation for Economic Co-operation and Development, 2010).*
[71] *(Pool Re, 2011).*

In 2007, the European Commission released a Business Insurance Sector Inquiry Report[72]. It noted that for business insurance EU insurers collect €375bn in non-life premiums every year. Compare this with the US market size quoted in the Betterly Report (of €620m in 2011) and it seems that the niche cyber-insurance market is still relatively small.[73]

The European Commission's interim report noted that when classifying the market by consumer segment, small business risks are offered in a similar way to personal lines of insurance on a commoditised basis. For larger firms, which are complex and unique in their characteristics, tailor made insurance solutions are necessary. This report classifies risks covered by business insurance into:

- ✓ Material damage (property insurance);
- ✓ Financial loss (pecuniary insurances) – financial losses beyond the cost of restoring the property itself, including legal expenses insurance and business interruption insurance;
- ✓ Liability insurances where a firm or individual who causes wrongful harm to others is liable in law to pay compensation including professional negligence or mis-management (professional indemnity insurance, directors and officers insurance and other special types).

Out of the range of types of insurance covered in this study, property/business interruption and liability (including general liability; professional indemnity and directors and officers' liability) are of specific interest.

According to European Commission Sector Inquiry Insurance Report, in 2007 there were 3,000 non-life insurance companies operating in Europe with average premium volumes around €125m each per firm.

Professional indemnity insurance was worth almost €6bn across Europe in 2010, according to a report from Insurance Insight.[74] It was estimated that this could grow to as much as €7bn by 2014. In ten major countries (Belgium, France, Germany, Poland, Spain Sweden, Switzerland and the UK) professional indemnity insurance was worth €5.81bn in 2010 in terms of gross written premiums. The total biggest category was healthcare, which is believed to account for over €2bn of the premiums paid.

By way of comparison, a 2009 report for the European Union by Europe Economics, considered the size of the European 3rd party liability motor insurance market the comprehensive motor insurance and the home/household insurance market. This indicated that although the motor insurance market did not exhibit real growth since 2005 in 2008 it accounted for just under €119bn. The home insurance market stood at €74bn in 2008.[75]

---

[72] *COM (2007) 556, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Sector Inquiry under Article 17 of Regulation (EC) No 1/2003 on business insurance.*

[73] *(Betterley, 2011).*

[74] *(Finaccord, 2011).*

[75] *European Economics, 2009.*

Secondary issues

Other concerns that have been elaborated include the aforementioned properties of moral hazard and adverse selection, stemming from information asymmetries, which characterise cyber-security more generally. In the case of moral hazard, firms may be motivated to act in a more risky fashion once an insurance contract is concluded because they have seemingly 'dealt' with the risks. They can do that because insurers cannot determine the relative effectiveness of security measures due to the reasons proposed above in the section on the visibility of measures – namely that there is asymmetry in the information available in both supply and demand in favour of the prospective insured. Secondly, the lack of information available on risks and exposure by firms creates an asymmetry in the opposite direction, resulting in adverse selection: put simply the insurer cannot sufficiently segregate its market, resulting in premiums being priced sub-optimally. There may be also regulatory issues including for example uncertainty about limitation of Internet Service Providers liability and other regulatory issues.[76]

There are also other reported considerations from the market itself [77]– for example, known risk (related to the question of adverse selection and asymmetric information where the insurer cannot determine to what level of risk a prospective insured is already exposed; the retroactive date of policies, measurement of the number of occurrences (how to determine one discrete security breach) and the 'long tail' or length of time claims could extend[78]. Known risk refers to the risky behaviour or cyber-risks present in the prospective insured that the insured doesn't know about, prior to taking out insurance. For example, since the question of whether some types of cyber-security risk can be fully identified (e.g. dormant threats, cyber-espionage or determined adversary) might inhibit the insurers offering products for fear of unlimited liability. This is also related to uncertainties about when policies would take effect and the possible length of time when risks can be identified and claims made. There is also finally the question of disaggregating what is actually a discrete, separate incident – should a denial of service for example, be 'counted' by the number of bots launching the attack, or by the number of C&C servers?.

[76] *CEPS, 2010.*
[77] *Perrin Conferences, 2012.*
[78] *For example, there are still cases being heard about health problems relating to asbestos some 40-50 years after the 'risk' was first discovered.*

Cyber Insurance market incentives

The promise of cyber-insurance reflects an understanding that it can offer benefits and desirable outcomes identified from analogy to other markets (e.g. fire insurance) that includes:[79]

- ✓ Incentives for firms to increase IT security in order to reduce premiums – assuming that it is possible to determine a causal link between certain information security measures and reduction in risk and that this information was readily available to the market and that such a link was taken into consideration by insurers when pricing premiums, then the prospective insured might be more inclined to evaluate their cost benefit trade-offs in favour of spending on security since the consequent likely reduction in premiums might offer greater cost savings;
- ✓ Processes to set IT security standards for underwriting – whilst IT security standards such as Common Criteria and the ISO 2700x series have been around for some time, the link between how these standards are developed and the insurance community might be strengthened by a more substantial market for cyber-insurance especially with greater involvement of the underwriting community;
- ✓ Security consulting firms that can investigate security practices as a part of the underwriting process – following on from above, there may be a market for firms offering security consulting and expertise in support of either underwriting or claims cases;
- ✓ Certification of IT security products and services – from a technical perspective inclusion and recognition of certain IT security products and services as reducing the premiums might at the least send a signal to the broader market about the relative effectiveness of certain security products and services thereby contributing to spill-over effects in the broader non-insured community;
- ✓ Incentives and means to promulgate best practices – as above, the insurance market could act as a mechanism or platform for the broader promulgation of best practices about what are worthwhile security practices;
- ✓ Incentives to keep responsibility and costs for addressing some cyber-security risks within the private sector – finally, the market can contribute to overall social welfare by helping to keep the costs for poor cyber-security within the private sector and not shifting costs and liability back onto the public sector.

[79] *(Baer, 2003).*

Incentives to cyber-insure may be classified into two types[80]:

- ✓ Subjective rationality when insurance permits the transfer of risk namely the exchange of future uncertain costs (costs of dealing with a breach, reputational damage or fines from regulators), provides for manageability (smoothing out of the costs associated with managing risks) and quantification (the premiums constitute a metric for the value of security);
- ✓ Substantial rationality when the demand for lower premiums may in turn stimulate implementation of more secure technologies from ICT providers; may stimulate demand from firms because this pays off in lower premiums; insurance provides an incentive to implement effective security measures and finally it spurs further research and development in those providing security technologies.

Broadly, the main incentives in the cyber-insurance domain can be linked to the expectations of firstly a better determination of what is effective in reducing risk (and therefore making users of such products and services a better risk for the insurance carriers) which in turn would stimulate a range of secondary markets, driving up supply and possibly raising the awareness of customers of the requirement to address cyber-security.

[80] *(Böhme and Kataria, 2006).*

Recommendations

We propose four recommendations based on what we have been able to discern from the theoretical issues identified above. It is important to note that our study was not empirically based but rather an exploratory investigation into this domain, therefore our recommendations are intended more as avenues for further investigation.

Collect empirical evidence as to the take up of cyber-risk insurance in Europe

Böhme and Schwartz conclude in their paper that although their analysis is based on analytical models of cyber-insurance, little quantitative empirical work exists on markets with respect to prices, volumes or losses.[81] They conclude that the positive expectations about cyber-insurance have not been thoroughly analysed and conclusions remain based on weak evidence even after a decade of theoretical research.

They argue that the rapid discounting of the validity of cyber-insurance has deterred further investigations. A useful preliminary step could be to investigate the relative claims of firms submitting cyber-risk related claims under existing and more general business insurance contracts (for example, D&O liability and business interruption). One such proposal would be to develop a survey on cyber-insurance to solicit empirical evidence such as:

- ✓ Knowledge of cyber-insurance market
- ✓ Types of risk insured;
- ✓ Types of loss insured (e.g. first or third party or indirect losses);
- ✓ Premiums;
- ✓ Pay-outs;
- ✓ Tort liability
- ✓ Risk metrics
- ✓ Enforcement
- ✓ Collective actions

Progressing this recommendation might be included in the efforts of underwriters and firms/organisations and data breach competent Authorities.

Explore understanding of opportunities for collective action or redress

The second recommendation is linked to the question of the regulatory landscape for collective action in Europe. In the narrow instance of the context of loss of personal data, it would appear that opportunities for victims to instigate collective action are limited as this would interfere with the interpretation of personal data as a fundamental human right rather than a property right that can be traded. This is shown by research, listing the authorities competent to undertake collective actions in the Member States, which does not include Data Protection Authorities.[82]

[81] *(Böhme and Schwartz, 2010).*
[82] *(Stuyck et al, 2007).*

The updating of European consumer rights legislation to strengthen the regulatory framework in the context of information society services could perhaps be one route to encouraging firms to take measures to improve their own risk management practices rather than primarily investing in cyber-insurance as a means to manage reputational damage arising from news about a data loss. The effects might be different whether there is a fault based tort liability (requiring common metrics and taxonomies of risk to determine who was at fault) or a mechanism of strict liability (where fines are issued from a regulator). In the former case, the impact on the cyber-insurance market would perhaps be a broader range of targeted products and greater choice on the demand side. Initial fact finding within the European Commission would be a preparatory step to understanding the current landscape in this regard.

Consider frameworks to help firms appraise the value of their information

A third and relatively simple recommendation would be to consider disseminating frameworks about the measurement of value of information. Information management/ information resource management (IRM) is the first step of a standard risk management approach, where an inventory is performed of what information an organisation thinks is critical. Greater understanding of how to measure and perhaps value or 'price' information assets may result in risk managers being able to better consider the role of insurance as a tool to support their activities. Such frameworks would also help the underwriting business. Indeed, one might imagine a situation where underwriters use kite-marked guidance to help them value their information. This would assist underwriters in pricing premiums and addressing claims.

As a further stage, specialised privacy and information security advisors can support the activities of underwriters, claims assessors or loss adjustors. The next step for this would be to collect best practices on information management and approaches to valuing non-tangible assets like information (parallels could perhaps be drawn with respect to how intangible assets are valued through patents, for example). This recommendation could be further explored by privacy and information security advisors, underwriters and the European Commission. ENISA could also provide support and suggestions.

Explore the role of government as insurer of last resort

Finally, as has been shown with the question about unlimited liability, there may be scope for public policy to intervene by setting itself as an insurer of last resort. This might build upon terrorism re-insurance as a model, an idea proposed by Mainelli (2012).[83] However, there would remain challenges to implementing this. Not least that attribution of a systemic cyber-risk (such as an act of cyber-terrorism or nation-state sponsored cyber-attack) that would affect all parties equally thus outside of the control of the insured and hence under the scope of a government re-insurance is difficult but not impossible. Here, the question of attribution comes into play and how to determine events that affect a single company, complete sector

[83] *Mainelli, M. (2012).*

or society as a whole. Compare this to physical terrorism in the real world where the distinction of what crosses a terrorism threshold is clearer thus making it more obvious when a government intervention programme would need to be activated. Collecting data on such re-insurance activities across the EU Member States in other contexts (e.g. in the domain of terrorism). This recommendation could be investigated by Member States and the European Commission.

In conclusion, we have seen that there exists a deal of uncertainty about the cyber-insurance market and about whether the theoretical barriers identified actually play a role. There appears to be contradictory evidence in this regard. On the one hand, economists and those studying the economics of information security[84] argue that these barriers are preventing a market from developing. On the other hand, there are indications that this market does exist and there are offerings and firms both supplying and demanding cyber-insurance.

Further exploration of this gap, along with some simple 'quick-wins' might be worthy of further consideration, under the caveat that they would not claim to 'solve' a problem of which we are still uncertain actually exists.

[84] *E.g. see the Workshop on the Economics of Information Security series.*

References

Advisen (2011) *'A new Era in Information Security and Cyber Liability Risk Management'* Advisen Ltd http://corner.advisen.com/pdf_files/cyberliability_riskmanagement.pdf

Attisani, D. (2012) Cyber Liability and Data Protection Issues presentation given at Perrin Conference Emerging Risks on Dual Frontiers: Perspectives on Potential Liabilities in the New Decade. London April 12 2012

Baer, W. S. (2003) *'Rewarding IT Security in the Marketplace'* Contemporary Security Policy,

Bandyopadhyay, T. M., Vijay, S. and Rao, Ram C (2009) *'Why IT Managers don't go for cyber-insurance products'* Communications of the ACM, 52(11), pp 68-73

Betterley, R. S. (2011) 'The Betterly Report: Cyber/Privacy/Media Liability Market Survey 2011' Sterling, MA:

Böhme, R. and Kataria, G. (2006). Models and measures for correlation in cyber-insurance. Paper presented at the Workshop on the Economics of Information Security.

Böhme, R. and Schwartz, G. (2010). Modeling Cyber-Insurance: *Towards a Unifying Framework, Working Paper. Harvard: Workshop on the Economics of Information Security* (WEIS) Harvard, June 2010.

Campbell, K., L.A., G., Loeb, M. P. and Zhou, L. (2003) *'The economic cost of publicly announced information security breaches: Empirical evidence from the stock market'* Journal of Computer Security, 11(3), pp 431-438

Cavusoglu, H., Mishra, B. and Raghunathan, S. (2004) *'The effect of a security breach announcement on market value: Capital market reactions for breached firms and Internet security developers'* International Journal of Electronic Commerce, 9(1 (Fall 2004)), pp 69-104

Centre for European Policy Studies (2010) Protecting Critical Infrastructure in the EU: CEPS Task Force Report; Brussels. Retrieved from: http://www.ceps.eu/ceps/download/4061

Chubb (2011). Chubb launches cyber security insurance http://www.chubb.com/international/uk/corporate/chubb14809.pdf

CIO.com (2012). EU's data protection proposals likely to include 24-hour breach notification http://www.cio.com.au/article/413120/eu_data_protection_proposals_likely_include_24-hour_breach_notification/

Claims Journal (2011). 9/11's Costly Insurance Impact http://www.claimsjournal.com/news/national/2011/09/09/190969.htm

European Commission (2007) *'Interim Report of Inquiry into the European business insurance sector pursuant to Article 17 of Regulation 1/2003'* Brussels: http://ec.europa.eu/competition/sectors/financial_services/inquiries/interim_report_24012007.pdf

ENISA (2011) *'Technical Guidelines on Implementing Minimum Security Measures: Guidance on the security measures in Article 13a Version 1.0,* December 2011'

Finaccord (2011). Professional Indemnity Insurance in Europe. Retrieved from http://www.finaccord.com/press-release_2011_professional-indemnity-insurance-in-europe.htm

Force, R. Davies, M. and Force, J. S. (2011) Symposium: Deep Trouble: Legal Ramifications of the Deepwater Horizon Oil Spill: Deepwater Horizon: Removal Costs, Civil Damages, Crimes, Civil Penalties, and State Remedies in Oil Spill Cases Tulane Law Review Vol 85 (889)

Fordayce, S. (1985) *'Insurance for Space Systems'* IEEE Journal on Selected Areas in Communications Vol 3 (1) pp 211 – 214

Foster, H. (1971) Employers Strike Insurance; Labor History Vol 12(4) pp 483-529

Georgia Tech Emerging Cyber Threats Report 2012. Retrieved from: http://gtisc.gatech.edu/doc/emerging_cyber_threats_report2012.pdf

Greisiger, M. (2011) 'Cyber Liability & Data Breach Insurance Claims - A Study of Actual Payouts for Covered Data Breaches' Gladwayne: NetDilligence

The Guardian (2011) Sony Suffers second data breach with theft of 25m more user details. Retrieved from http://www.guardian.co.uk/technology/blog/2011/may/03/sony-data-breach-online-entertainment

Hartwig, R. P. and Wilkinson, C. (2011) *'Social Media, Liability and Insurance'* New York: Insurance Information Institute

Heal, G, Kearns M, Kleindorfer P and, Kunreuther, H (2006) '*Interdependent Security in Interconnected networks* 'Insurance Journal (2012) Chartis Introduces CyberEdge Tower April 4 2012. Retrieved from: http://www.insurancejournal.com/news/national/2012/04/04/242161.htm

Insurance Networking News (2012) Insurance Industry Responds to Cyber Attack Increase. April 20, 2012 retrieved from: http://www.insurancenetworking.com/news/cyber-insurance-standards-zurich-cna-liberty-30256-1.html

Insurance Services Office (2009), Information Security Protection Policy EC 00 10 11 09

Ko, M. and Dorantes, C. (2006) *'The impact of information security breaches on financial performance of the breached firms: an empirical investigation'* Journal of Information Technology Management, XVII(2), pp 12-22

Kunrether, H. and Heal, G. (2003) *'Interdependent Security'* Journal of Risk and Uncertainty, 26(2-3), pp 231

Lloyds (2011). Rising claims reflect cyber concerns of multi nationals. News and Features: Market News,

Mainelli, M. (2012) Cyber Re - A Reinsurance Proposal For National ICT Infrastructure Security & Competitiveness, ZYen; London. Retrieved from: http://www.zyen.com/what-we-do/research-proposals.html

Mankabady, S. (1985) The Development of Offshore Insurance law Journal of Maritime Law and Commerce Vol 16(1) pp 101-113

Mehr R. and Cammack, E. (1980) Principles of Insurance (7th ed). R.D. Irwin; Homewood, IL

Organisation for Economic Co-operation and Development (2010). Conference on Terrorism Risk Insurance http://www.oecd.org/document/52/0,3746,en_2649_34851_45023412_1_1_1_1,00.html#Documentation

Pal, R. (2012) Cyber-Insurance in Internet Security Digging into the Information Asymmetry Problem unpublished paper; retrieved from http://arxiv.org/pdf/1202.0884.pdf

Perrin Conferences (2012) *Emerging Risks on Dual Frontiers: Perspectives on Potential Liabilities in the New Decade*. London April 12-13.

Pool Re (2011) 'Welcome to Pool Reinsurance' London: Pool Reinsurance Company Limited http://www.poolre.co.uk/PoolReinsurance.pdf

President's Working Group on Financial Markets (2010) 'Report of the President's Working Group on Financial Markets: Market Conditions for Terrorism Risk Insurance 2010' Washington DC:

PwC (2010) 'Global State of Information Security Survey' London: http://www.pwc.com/en_GX/gx/information-security-survey/pdf/pwcsurvey2010_report.pdf

Rue, R., Pfleeger, S. and Ortiz, D. 2007 '*A Framework for Classifying and Comparing Models of Cyber Security Investment to Support Policy and Decision-Making* '. Proceedings of the Sixth Workshop on Economics of Information Security, Pittsburgh PA.,

Schoenberger, C. R. (2001). Payout. Forbes.

Shetty, N. S., Galina; Felegyhazi, Mark and Walrand, Jean (2010) 'Competitive Cyber-Insurance and Internet Security. '. In Tyler. Moore, D. P., and Christos. Ioannidis (ed) Economics of Information Security and Privacy, pp 229 - 247. Springer-Verlag.

Stuyck, J., Terryn, E. Colaert, V., Van Dyck, T. Peretz, N., Hoekx, N. and Tereszkiewicz, P. (2007) An Analysis and *Evaluation of the Alternative Means of Consumer Redress Other Than Redress Through Ordinary Judicial Proceedings, Final Report: A Study for the European Commission, Health and Consumer Protection* Directorate-General Directorate B-Consumer Affairs; Study Centre for Consumer Law, Centre for European Economic law, Katholieke Universiteit Leuven, Belgium. Retrieved from: http://ec.europa.eu/consumers/redress/reports_studies/comparative_report_en.pdf

The Security Blog (2011) Revealed: Operation Shady RAT. Retrieved from: http://www.thesecurityblog.com/2011/08/revealed-operation-shady-rat/

Yurcik, W. and Doss, D. (2002). Cyber insurance: A market solution to the internet security market failure. Paper presented at the Workshop on the *Economics of Information Security.*

Weiss, M. A and Manikowski, P. (2007) The Satellite Insurance Market and Underwriting Cycles presentation at the American Risk and Insurance Association Annual Meeting Quebec City, Quebec August 2007

Appendix A– Academic Research

In this appendix we provide an overview of some relevant academic papers which discuss theoretical solutions to the apparent failure of the cyber-insurance market.

(Yurcik and Doss, 2002) propose that cyber-insurance is a market solution to the failure of Internet security.

(Böhme and Kataria, 2006) discuss a two-step model for risk arrival which includes consideration of correlated risk within a firm (failure of systems internally to the firm) and global correlation (failure across multiple firms in an insurers portfolio). These two types of correlation affect the supply and demand sides: internal correlation may influence firms' decision to seek insurance whilst external correlation may influence the premium set by insurers.

Others (Bandyopadhyay, 2009) indicate that obstacles in the demand side present the most likely explanations for the current poor market. They argue that since insurers are unable to determine the likely secondary losses from customers (the amount arising from losses such as regulatory fines, downstream liability etc. They find that because insurers do not have better information on the secondary losses leading to the perception from the firm that there will be too little expected indemnity from a product because of the high overall deductible (regardless of if there were primary or secondary losses). This under claiming strategy thus compounds the characteristic of information asymmetry in the market: the insured do not claim, leading to the insurers being unable to accurately price products at a firms' level would find attractive. The proposed premium structure is regarded as overpriced because firms apply a strategy to under claim based on appreciation of their secondary losses, causing them to find the product overpriced. They conclude that firms with IT intensive business processes would prefer to self-insure a high proportion of their cyber risk, whereas firms with low intensity or reliance upon IT may find insurance products less expensive (and more attractive) under today's market conditions.

(Shetty, 2010) find that a market for competitive cyber-insurance is lacking and additionally fails to improve network security since insurers cannot observe the security behaviour of users. They investigate in a model of user and network heterogeneity, how information asymmetry affects the insurance market, finding that in the presence of perfect information between insurers and insured, user utility is higher but network security is not. Network security in fact may be lower with insurance because of the moral hazard problem (insured invests less in security measures due to the presence of insurance). They identified that although insurance improves the utility for risk averse to users it does not "serve as an incentive device for improving security practices" since insurance is for risk management and redistribution and not risk reduction. However, this is rather different to other established literature defining the utility of insurance as a means to firstly: transfer the financial consequences of risk (and not necessarily the technical risk) and secondly insurance as a way to transfer residual risk (i.e. after all other security mechanisms have been applied).

This framework is then systematically applied to a literature review in the context of three research questions:

- ✓ What conditions inform the growth of the market and what is driving its failure?
- ✓ What is the effect of a market on aggregate network security? Will security improve if cyber-insurance is broadly adopted?
- ✓ Does cyber-risk reallocation contribute to social welfare?

The authors find nine papers describing technical models of market based cyber-insurance worthy of further explanation. They conclude that these papers present some intuitive insight into specific aspects including that in general cyber-insurance does not necessarily contribute to improved network security (socially optimum levels). The possibilities for re-allocation of risk via cyber-insurance described in the models reviewed help in reducing firms propensity to overinvest in security measures but the newly available resources are not deployed in further security measures but rather other 'more productive activities'.

Finally, five key components of cyber-insurance are highlighted in an economic model proposed as a unifying framework (Boehme and Schwartz in 2010):

- ✓ Network environment – a model which takes account of the aspects of interdependent security and correlated risk described above which encompasses nodes controlled by agents;
- ✓ Demand side – agents (those prospective organisations considering insurance decisions);
- ✓ Supply side – insurers;
- ✓ Information structure – all decisions gathered about the distribution of knowledge amongst the players which includes aspects of information asymmetry identified above;
- ✓ Organisational environment – various public and private entities that affect network security and agents security decisions (including government policy).

P.O. Box 1309, 71001 Heraklion, Greece
www.enisa.europa.eu