Cyber Security Policy and Research Institute

THE GEORGE WASHINGTON UNIVERSITY

Insurance for Cyber Attacks: The Issue of Setting Premiums in Context

Costis Toregas

Nicolas Zahn

January 7, 2014

Report GW-CSPRI-2014-1

Insurance for Cyber Attacks: The Issue of Setting Premiums in Context

Costis Toregas
Nicolas Zahn

Abstract

With the steady increase in cyber attacks, more companies are looking to the developing cyberinsurance market for relief. Although many arguments have been made in its favor, the cyberinsurance market faces various challenges, with the setting of premiums being one of the biggest issues. This paper will draw from the body of existing literature and a set of newly conducted interviews to present an overview of the current cyberinsurance market. This overview will also discuss the barriers that hinder cyberinsurance's development into a mature market. Lastly, this paper will illustrate the potential for collaboration between the private sector and academia and suggest a research agenda to for the setting of cyberinsurance policy premiums.

Introduction

Cyber attacks pose considerable risk for many companies. They cause business interruptions due to Denial of Service attacks and can result in the loss of intellectual property and business secrets. Potential losses include: merger plans, loss of customer data coupled with reputational damage and possible litigation costs etc.[1] According to the Identity Theft Resource Center, 17,491,690 records where breached in 2012.[2] A 2013 study by the Ponemon Institute showed that 28,765 records were breached per incident on average in the US alone, resulting in more than $5 million worth of damages. Malicious or criminal attacks were the most costly data breaches in the surveyed countries.[3] With the e-commerce market being worth $7 trillion, it is a particularly lucrative target for cyber attacks.[4] The effects of cyber attacks could be detrimental to businesses who operate mostly in online sales: potential attacks against online retailers during "Cyber Monday" of 2013 could lead to a loss upwards of $3.4 million per hour.[5] Looking beyond a data breach, the damage experienced by companies increases to more than $9 million.[6] On top of monetary damages, companies also face a number of potential cyber-related adversaries: from disgruntled employees, "hacktivists" and competitors to state agents.[7]

While there is active discussion as to the methodology and terminology used in identifying and quantifying the costs and risks associated with cyber attacks,[8] it has become clear that more companies are vulnerable to attacks like the ones mentioned above. 89% of respondents in a recent Advisen study on Information Security acknowledged that information security risks pose at least a moderate threat to their company.[9] This pending threat has generated a sense of worry among companies. Respondents to the 2013 Ponemon Cyber Insurance Report also felt financial losses due to cyber attacks would increase in the future.[10] Although some companies recognize the danger of such attacks, there seems to be a gap between these threats and companies having to deal with them. This disconnect may be from an unwillingness or inability to invest in adequate IT security.[11]

Furthermore, the spread of new technologies such as Cloud Computing, mobile devices, and social media increases vulnerability to cyber attacks, as the focus of customers' lies on using those technologies to enhance the efficiency of their business - not the security. Due to heavy competition, producers of such technologies also prefer to focus on fast product development, not necessarily the security of those products and services.[12] At the same time, more businesses have become increasingly reliant on storing massive amounts of data electronically, often using outsourcing or third-party software.[13]

---

[1] (Anderson, et al. 2012, 3); (Etzioni 2011, 58); (Friedman, Cyber Theft of Competitive Data: Asking the Right Questions 2013, 4f.); (Kesan, Majuca und Yurcik, The Economic Case for Cyberinsurance 2005, 2); (Nordman 2012, 28)

[2] (ITRC 2012)

[3] (Ponemon, 2013 Cost of Data Breach Study: Global Analysis 2013, 1-4)

[4] (ISO 2005)

[5] (PRNewswire 2013)

[6] (Ponemon, Manaing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age 2013, 4)

[7] (Conti, et al. 2013); (Hedrick 2007, 1)

[8] See generally (Friedman, Cyber Theft of Competitive Data: Asking the Right Questions 2013) and (Friedman, Economic and Policy Framework for Cybersecurity Risks 2011). On a discussion of how to measure costs of cybercrime see (Anderson, et al. 2012); (Brecht und Nowey 2012); (Capgemini 2012)

[9] (Advisen 2013, 3)

[10] (Ponemon, Manaing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age 2013, 4)

[11] (Etzioni 2011, 59); (MacWillson, et al. 2011); (Phelps, van den Dool und O'Rourke 2012, 2). For a discussion of the perception of IT security see (Ryan 2011)

[12] (Friedman, Economic and Policy Framework for Cybersecurity Risks 2011, 9f.)

[13] (Hedrick 2007, 1); (A. MacWillson 2012, 2f.)

Facing those threats, companies have developed an increasingly sophisticated supply of technologies and services. These include firewalls and encryption over specialized personnel to specific cyberinsurance policies. This paper takes a closer look at the cyberinsurance market in the United States, how it has evolved, and what challenges it faces. Based on existing literature as well as a number of interviews,[14] it puts the question of how to set premiums for cyberinsurance policies in context and identifies it as one of the key challenges for a more mature cyberinsurance market. The goal of this paper is to get people from academia, the insurance industry, and companies interested in cyberinsurance thinking about the current challenges. The paper will conclude with a research agenda.

Dealing with cyber attacks

New technologies have helped to increase efficiency and productivity and have also created new business models. However, there is no denying that they have also created new threats to companies. Cyber attacks can have a devastating impact on a company: a study found that the average financial impact of a cyber attack was $9.4 million and that future attacks could potentially result in costs as high as $163 million.[15] As the market for e-commerce alone was valued at $7 trillion back in 2005, there is great potential for more costly attacks.[16]

Hence companies have to come up with responsive ways of dealing with cyber attacks. Similar to other risk management areas there are three basic strategies: self-protection, self-insurance, and transfer of risk through (cyber)insurance.[17]

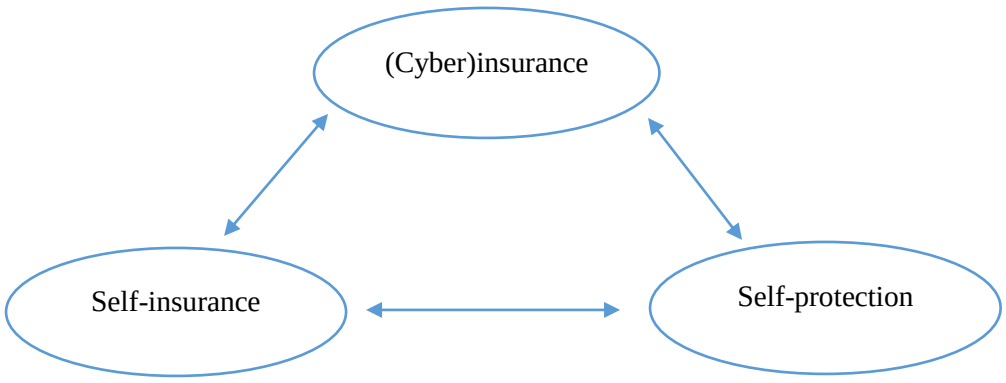

Figure 1: Strategies to deal with cyber-risk (adapted from Kesan, Majuca, Yurcik 2004:13)

As Figure 1 shows those strategies offer discrete ways of dealing with the risk of cyber attacks but can also work together in a mix. *Self-protection* refers to investments made to lower the risk of an attack such as IT security infrastructure, policies, e.g. encryption, and raising awareness among employees. However, investment in self-protection measures has been found to be too low and ill-conceived, leading to

[14] Concrete findings will be referenced as (Toregas and Zahn, Interviews 2013). For a summary of the findings as well as the methodology see Interview Outcomes.
[15] (Ponemon, Managing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age 2013, 1).
[16] (ISO 2005)
[17] (Capgemini 2012, 7); (ENISA, Incentives and barriers of the cyber Insurance market in Europe 2012, 13); (Gordon, Loeb und Sohail 2003, 84); (Kesan, Majuca und Yurcik, Cyberinsurance As A Market-Based Solution To The Problem Of CyberSecurity - A Case Study 2005, 9) There is also a fourth fallback option of accepting risk, see (Hedrick 2007, 2); (Innerhofer-Oberperfler und Breu 2010, 250)

sometimes perverse incentives, e.g. bad configuration of otherwise useful systems.[18] Self-protection also includes so-called 'active defenses', where a company that has fallen victim to a cyber attacks takes active steps against a perpetrator, e.g. "hacking back".[19] Under the current legal framework such steps are, discouraged and it is far from clear that such measures will work.[20]

A consensus is growing that IT security is not achievable by solely focusing on technological aspects. The present risk of cyber attacks is "essentially a business problem."[21] Hence, in addition to lowering the likelihood of cyber attacks through mostly technical means, companies can try to absorb losses incurred by such attacks through *self-insurance*, i.e. setting aside funds. Of course, this would necessitate the ability to judge and adequately quantify the risks and the availability of sufficient resources. Depending on the size and capabilities of the company, this might prove difficult or even impossible.[22] Finally, the risk can also be transferred through a specific *cyberinsurance* policy. In that case, the insurer agrees to bear the losses incurred by cyber attacks and receives a recurring policy premium in return. Companies need to understand the extent of their current coverage and identify possible vulnerabilities in order to choose an adequate cyberinsurance policy.[23]

Ideally, companies deal with the risk of cyber attacks by using a combination of the above mentioned methods.[24] But how do managers make their choices about how much they should invest and in what strategy? First, managers need facts about the risk of cyber attacks and the three possible mitigation strategies. Second, based on those facts and the incentives they face, managers will make a decision. To appeal to "business people," people in charge of IT have to translate the risks of cyber attacks into numbers and provide objective information instead of the common "fear, uncertainty and doubt" tactic.[25] One measure of doing so is to provide a return on security investment (ROSI).[26] This measure takes into account that "security is not usually an investment that provides profit but loss prevention" and helps companies to answer such questions as: are we paying too much for our security? Is a specific security product/service beneficial? However, ROSI is not without its critics.[27]

The next step of decision-making investigates what incentives exist for individual companies to invest in one or all of the strategies. This is called the economic approach to information security.[28] We can understand risk mitigation of cyber attacks as a market - actors can invest in certain strategies to protect against attacks from other actors.[29] Within this framework of economic analysis we can assess the impact of different choices, e.g. what happens when companies get together and collaborate in the field of IT

[18] (Baer und Parkinson 2007, 50); (Schneier, Hacking the Business Climate for Network Security 2004, 88); (Varian 2000)
[19] (Santo, Starrs und Viale 2013, 14)
[20] (Conti, et al. 2013)
[21] (Bandyopadhyay, Mookerjee und Rao 2009, 68); (Böhme, Cyber-Insurance Revisited 2005, 1); (Capgemini 2012, 7); (Foster 2006); (Hedrick 2007, 2); (Phelps, van den Dool und O'Rourke 2012, 7); (Ryan 2011, 8); (Schneier, Hacking the Business Climate for Network Security 2004, 87)
[22] (Capgemini 2012, 7)
[23] (R. D. Anderson, Insurance Coverage for Cyber Attacks - Part One of a Two-Part Article 2013); (R. D. Anderson, Insurance Coverage for Cyber Attacks - Part Two of a Two-Part Article 2013); (Gordon, Loeb und Sohail 2003, 84)
[24] (Capgemini 2012, 17)
[25] (DHS 2013, 13, 15)
[26] (ENISA, Introduction to return on Security Investment - Helping CERTs assessing the cost of (lack of) security 2012)
[27] (ENISA, Introduction to return on Security Investment - Helping CERTs assessing the cost of (lack of) security 2012, 1f.); (Gordon und Loeb 2002); (Schneier, Hacking the Business Climate for Network Security 2004)
[28] (Friedman, Economic and Policy Framework for Cybersecurity Risks 2011, 5)
[29] (Cordes 2011); (Friedman, Economic and Policy Framework for Cybersecurity Risks 2011, 8)

security or what influence new government regulations, e.g. to disclose information about cyber attacks, have on the incentives of individual companies to invest in the security strategies.[30]

Focusing on incentives reveals not only options for companies, but also what role the government can play by changing those incentives, e.g. through new regulation.[31] However, governmental changes to the incentives can also create their own problems.[32] Insurance can provide for a market-based way of changing incentives towards more adequate security investment.[33] Hence, cyberinsurance is not only an interesting addition to the basket of mitigation strategies from a company's perspective, it is also interesting from a societal perspective, as it might improve the overall IT security.

Cyberinsurance: What are the Issues?

Arguments for and against Cyberinsurance

Cyberinsurance is defined as "the transfer of financial risk associated with network and computer incidents to a third party," the insurance company, in exchange for a premium.[34] Cyberinsurance policies are usually very client-specific and negotiated on a case-by-case basis.[35] They cover aspects not included in "traditional" insurance policies, e.g. liability arising from loss or theft of electronic data as well as regulatory fines.[36] Cyberinsurance policies are available for first-party and third-party coverage.[37]

Cyberinsurance policies offer benefits similar to insurance in other areas:[38]

1. Without the possibility of *transferring risks*, risk-averse companies and companies looking to bear risks do not find each other in the market place, resulting in market inefficiency. By providing the possibility of risk transfer, insurers create a sense of welfare, as companies can now transfer risk to willing parties.
2. Because insurers can differentiate between companies through rates premiums and (lower premiums for low-risk companies), insurers can *incentivize investment in IT security*. This market-based process facilitates the adoption of standards and metrics for IT security. It works as a driver for innovation, as companies demand ever more sophisticated ways of protecting themselves. If standards promulgated by insurers are accurate and correct, this benefit can bring improvements to the operations of cybersecurity with no regulatory intervention.

[30] (Cordes 2011, 10); (Elliott und Saka 2010, 16); (Kobayashi 2006)
[31] (Conti, et al. 2013); (Cordes 2011, 11); (Kobayashi 2006)
[32] (Kobayashi 2006, 277); (Kesan, Majuca und Yurcik, The Economic Case for Cyberinsurance 2005, 18). See (Etzioni 2011, 59) for a successful example of governmental action realigning incentives for security investment.
[33] (Baer und Parkinson 2007, 50)
[34] (Böhme, Cyber-Insurance Revisited 2005, 5); (Böhme und Schwartz, Modeling Cyber-Insurance: Towards A Unifying Framework 2010, 1); (Clinton undated, 1); (ENISA, Incentives and barriers of the cyber Insurance market in Europe 2012, 8)
[35] (Nordman 2012, 29)
[36] (Bandyopadhyay, Mookerjee und Rao 2009, 68)
[37] "First-party risk occurs when the insured faces the possibility of loss of profits. Third-party risks are those faced by the insured because of damages caused to another firm or individual. The most common types of first-party coverage include business interruption, electronic data damage, and extortion, while the most common third-party coverage include network security liability, downstream network liability, and media liability" (Hedrick 2007, 2)
[38] (Baer und Parkinson 2007, 51); (Böhme, Cyber-Insurance Revisited 2005, 2, 13); (Clinton undated, 1); (ENISA, Incentives and barriers of the cyber Insurance market in Europe 2012, 13); (Hedrick 2007, 3); (III 2003); (Kesan, Majuca und Yurcik, The Economic Case for Cyberinsurance 2005, 7, 19); (Kesan, Majuca und Yurcik, Cyberinsurance As A Market-Based Solution To The Problem Of CyberSecurity - A Case Study 2005, 17); (Wheeler 2013)

3. As demand for cyberinsurance increases, best practices spread through the economy. Insurance improves the systemic resilience of a national economy and distributes risk fairly. Hence, insurance would help to *boost IT security,* rather than government regulations.

From a practical perspective, there is a business case to be made for cyberinsurance. The losses incurred from cyber attacks are growing as new technologies spread and reliance on technology increases. The misperception by managers that cyber risks are covered by "traditional" insurance, e.g. commercial general liability (CGL), has resulted "in costly litigation wars between insurers and their policyholders."[39] Since insurers maintain that "network security risks are fundamentally different than traditional physical risks", e.g. they are non-tangible and global in nature, insurers have fought to exclude coverage from "traditional" policies. Instead, they offer stand-alone cybersecurity policies.[40]

There are also arguments against cyberinsurance and skepticism about its positive effects. Some believe that the risks associated with cyber attacks are not quantifiable and thus, not insurable (at least not to the degree promised by insurers).[41] Another point against cyberinsurance is that it may provide companies with 'an easy way out': instead of working on their security, they just buy insurance. [42] As shown below, insurers are well aware of this danger. Many participants at a government sponsored roundtable discussion expressed skepticism about the capabilities of insurers to provide appropriate incentives for better IT security.[43]

Evolution of the market and challenges

While there is disagreement about the exact birth date of cyberinsurance policies, it is clear that the market is relatively new and not yet mature.[44] Considering the potential benefits of cyberinsurance as outlined above, the first cyberinsurance policies sparked hopes that "cyberinsurance might become as important and as ubiquitous in the IT security toolbox as [...] firewalls and antivirus software."[45] Government officials also praised cyberinsurance as an important mechanism to increase IT security.[46] However, the growth of the cyberinsurance market has somewhat been tentative and slow, prompting experts to revise their initial forecasts for the evolution of the market.[47] Inadequate coverage by "traditional" policies, increased vulnerability, and exposure to cyber risks (as well as lack of resources to self-insure) should be driving the demand for cyberinsurance policies. Until recently, few companies planned to buy cyberinsurance policies and an even fewer number actually bought cyberinsurance policies.[48] Still, the market for cyberinsurance policies is here to stay and expected to grow in the future.[49]

---

[39] (Kesan, Majuca und Yurcik, The Economic Case for Cyberinsurance 2005, 5)
[40] (R. D. Anderson, Insurance Coverage for Cyber Attacks - Part Two of a Two-Part Article 2013); (Baer und Parkinson 2007, 51); (Duffy 2002); (III 2003); (Kesan, Majuca und Yurcik, The Economic Case for Cyberinsurance 2005, 5); (Nordman 2012, 28)
[41] (ENISA, Incentives and barriers of the cyber Insurance market in Europe 2012, 23); (Gralla 2001)
[42] (DHS 2013, 11); (Wheeler 2013)
[43] (DHS 2013, 4)
[44] (Baer und Parkinson 2007, 51); (ENISA, Incentives and barriers of the cyber Insurance market in Europe 2012, 1) ; (Hedrick 2007, 2)
[45] (Baer und Parkinson 2007, 56)
[46] (Clinton undated, 1); (Daniel 2013)
[47] (Bandyopadhyay, Mookerjee und Rao 2009, 68f.)
[48] (Foster 2006); (Friedman, Economic and Policy Framework for Cybersecurity Risks 2011, 13); (HBR 2013, 1-8); (Hedrick 2007, 3); (III 2003); (Kesan, Majuca und Yurcik, The Economic Case for Cyberinsurance 2005, 7); (Kesan, Majuca und Yurcik, Cyberinsurance As A Market-Based Solution To The Problem Of CyberSecurity - A Case Study 2005, 3); (Mello 2013); (Ponemon, Manaing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age 2013, 4); (Wood 2007)
[49] (Nordman 2012, 29)

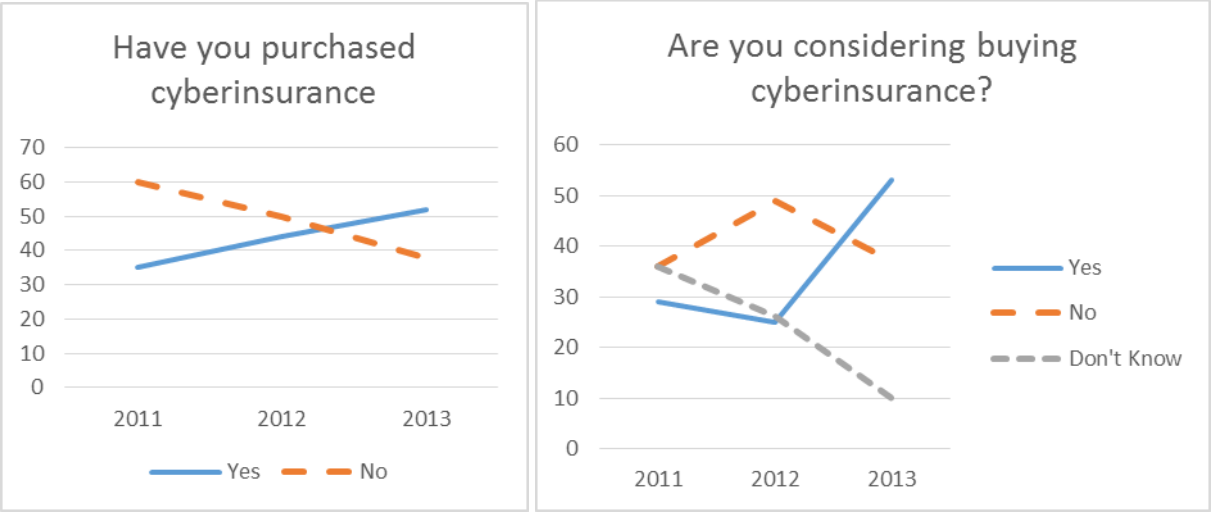

Figure 2: showing percentage of respondents (Advisen 2013, 7f.)

The latest trends seem to support this optimistic view: A recent Advisen report identified 2013 as a possible "cyber tipping-point," stating that after large firms were mostly aware of their risk exposure to cyber attacks, "smaller businesses began to increasingly realize that they were also at risk." This reflects that "insurance [had] cemented itself as a part of the cyber risk management strategy for a majority of companies surveyed by Advisen."[50] In line with these findings, a Ponemon Institute report showed that companies are concerned about future cyber attacks. This is likely to drive demand for cyberinsurance further in the future.[51] As Figure 2 shows, more companies are not only considering to buy cyberinsurance - they are buying policies. This is moving cyberinsurance "into the mainstream as a tool for managing IT security risks."[52]

Yet, the market for cyberinsurance still faces challenges, some comparable to other new insurance markets These challenges include:[53]

1. "traditional" insurance market challenges:
    a. information asymmetry
    b. moral hazard
    c. adverse selection

2. cyberinsurance challenges:

---

[50] (Advisen 2013, 2)
[51] (Ponemon, Managing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age 2013, 1f.)
[52] (Baer und Parkinson 2007, 54)
[53] (R. D. Anderson, Insurance Coverage for Cyber Attacks - Part Two of a Two-Part Article 2013); (Baer und Parkinson 2007, 52f.); (Bandyopadhyay, Mookerjee und Rao 2009, 68); (Böhme, Cyber-Insurance Revisited 2005, 13); (Capgemini 2012, 11); (Clinton undated, 2f., 5); (DHS 2013, 4, 8, 10, 12, 20); (Duffy 2002); (ENISA, Incentives and barriers of the cyber Insurance market in Europe 2012, 1f., 19, 21-24); (Friedman, Economic and Policy Framework for Cybersecurity Risks 2011, 11); (Gordon und Loeb 2002, 82); (Gralla 2001); (HBR 2013, 1); (Hedrick 2007, 3); (Herendeen, et al. 2012, 3); (Innerhofer-Oberperfler und Breu 2010, 250-253, 267); (Kesan, Majuca und Yurcik, Cyberinsurance As A Market-Based Solution To The Problem Of CyberSecurity - A Case Study 2005, 18ff.); (Kotulic und Clark 2004); (Kovacs, Markham und Sweeting 2004); (NetDiligence 2013, 22); (Ponemon, Managing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age 2013, 1, 4); (Ryan 2011, 6-8); (Schneier, Hacking the Business Climate for Network Security 2004, 88f.); (Wheeler 2013); (Wood 2007). While some challenges may relate to each other, they have been broken down into different categories for better clarity.

a. legal framework
    i. uncertainty about liability
    ii. spotty coverage and insurance loopholes
    iii. lack of standards or "bad" standards
b. conceptual issues
    i. quantification of risks and costs
    ii. cyber risk not seen as a business problem or underestimated
    iii. correlated, interrelated and global risks
    iv. lack of re-insurance
c. setting premiums
    i. lack of actuarial data
    ii. uncertainty about normative standards
    iii. premiums too high

Of course, not all issues are equally important and arguably, many will be resolved over time. For example: 2.b.ii: awareness is growing among business leaders that they are vulnerable to cyber attacks and need to do something about it. The three "traditional" insurance market challenges, information asymmetry, moral hazard and adverse selection, will not be discussed in this paper as insurers are familiar with these problems and have already gathered experience to deal with them in other markets.[54] In fact, many insurers are using sophisticated monitoring technology and other tools to overcome those challenges in the cyberinsurance market.[55]

The challenges under 2a affect companies, insurers, and the government (which is ultimately responsible for the legal framework). Liability rules have not caught up to the challenges new technologies create.[56] This prompts questions like: "should companies focus their cyber risk management efforts on patching vulnerable IT products, or should IT manufacturers and suppliers focus on poorly written code before bringing their products to market?"[57] Furthermore, coverage of cyber insurance policies remains very spotty, sometimes without companies realizing that a specific event is not covered. Policy exclusions have yet to face court judgments.[58] This can create the impression that insurers will always find a pretext for reneging on their commitments.[59] Small and middle-sized companies also fall victim to multiple problems, such as compliance with regulatory standards and getting insurance.[60] Repeated dialogue and cooperation between the stakeholders could create more clarity and alleviate those challenges.

The challenges under 2b provide a number of interesting questions for further research, many of which effect insurance companies.. As stated in the introduction, both stakeholders have difficulties quantifying risks and costs, be it for investments in IT security or for losses incurred through cyber attacks.[61] Even today, cyber risks seem hard to understand for risk managers and the task of dealing with cyber risks is

[54] For further reading see (Bandyopadhyay, Mookerjee und Rao 2009); (ENISA, Incentives and barriers of the cyber Insurance market in Europe 2012); (Gordon, Loeb und Sohail 2003); (Hedrick 2007); (Kesan, Majuca und Yurcik, Cyberinsurance As A Market-Based Solution To The Problem Of CyberSecurity - A Case Study 2005)
[55] (DHS 2013, 29); (Gordon, Loeb und Sohail 2003, 83); (Hedrick 2007, 3); (Kesan, Majuca und Yurcik, Cyberinsurance As A Market-Based Solution To The Problem Of CyberSecurity - A Case Study 2005, 14, 20)
[56] (Baer und Parkinson 2007, 55); (Böhme, Cyber-Insurance Revisited 2005, 13); (Ryan 2011, 6f.)
[57] (DHS 2013, 10)
[58] (R. D. Anderson, Insurance Coverage for Cyber Attacks - Part One of a Two-Part Article 2013); (R. D. Anderson, Insurance Coverage for Cyber Attacks - Part Two of a Two-Part Article 2013); (ENISA, Incentives and barriers of the cyber Insurance market in Europe 2012, 21); (Wood 2007)
[59] (Toregas and Zahn, Interviews 2013)
[60] (DHS 2013, 20)
[61] (NetDiligence 2013, 22); (DHS 2013, 3, 8); (Mello 2013). See also *supra note* 8.

often transferred to the IT department of a company.[62] As stated, this is changing and future risk managers are likely to better understand cyber risks and what cyberinsurance can contribute to their risk management strategy. Insurers, on the other hand, are faced with risks that are potentially correlated and interrelated as well as global in nature. For example, some technologies, e.g. operating systems, are used by a wide number of companies all over the world.[63] Consequently, one vulnerability exploited by a hacker can lead to a very high number of losses, even in companies that are not directly targeted by a cyber attack. This in turn creates the next challenge: how will a company deal with potentially very high losses, or "cyber hurricane"?[64] In other markets, re-insurance mechanisms or backstops exist that provide insurers with a way out in cases of extraordinarily high claims. This is not (yet) the case for cyber attacks. To address this issue, several proposals have been put forward, most notably the establishment of a backstop fund similar to the Terrorism Risk Insurance Act (TRIA).[65]

The issue of setting premiums in context

A final set of challenges relates to the process of setting premiums. Currently, this is weakened by a lack of actuarial data and uncertainty about normative standards. This has led to high costs for insurers and in turn, high premiums that deter companies from buying cyberinsurance.

There are two ways of determining premiums: through actuarial data and normative standards. With actuarial data, insurance companies are looking at past events to determine how likely they are in the future. Sophisticated statistical models exist to determine this likelihood based on a number of factors for mature insurance markets, e.g. car insurance.[66] With normative standards, insurance companies base their calculations on causal relationships between various factors, e.g. someone who never exercises is more likely to suffer from Diabetes. Both ways ultimately tell the insurance company how likely a loss event is. The lower this likelihood, the lower the premium for the policy.[67] In the absence of either possibility, insurers are "left to their own underwriting standards and creativity" and can offer policies for any premium the "market will bear."[68]

Given that many companies are either unaware of a cyber attack or unwilling to disclose such attacks, and added to the fact that those attacks are hard to quantify, actuarial data for the cyberinsurance market is missing and unlikely to be available in the near future.[69] Normative standards, i.e. certain types of behavior, help indicate a certain risk level for a cyber attack. The question of what constitutes 'good IT security' has not been answered conclusively.[70] This is not to say, however, that insurers and companies are completely clueless about their IT security. For example, there are certain standards on IT security , like ISO/IEC 27000 – but the underwriting procedures for cybersecurity policies are not fully harmonized

---

[62] (Advisen 2013, 5); (Bandyopadhyay, Mookerjee und Rao 2009, 68); (DHS 2013, 12); (HBR 2013, 1); (Ponemon, Manaing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age 2013, 1)

[63] (Baer und Parkinson 2007, 53); (Böhme, Cyber-Insurance Revisited 2005); (Pasciullo 2008)

[64] (Baer und Parkinson 2007, 54); (Clinton undated, 2f.); (Duffy 2002); (ENISA, Incentives and barriers of the cyber Insurance market in Europe 2012, 2)

[65] (Clinton undated, 4ff.); (Homeland Security News Wire 2013)

[66] The website of the National Association of Insurance Commissioners offers a look at a model for car insurance: http://www.naic.org/documents/committees_c_100930_presentation_iso.pdf

[67] (Foster 2006); (Gordon, Loeb und Sohail 2003, 82)

[68] (Foster 2006); (Mello 2013); (Wheeler 2013)

[69] (Bandyopadhyay, Mookerjee und Rao 2009, 73); (Capgemini 2012, 11); (Duffy 2002); (ENISA, Incentives and barriers of the cyber Insurance market in Europe 2012, 1, 19); (Hedrick 2007, 3); (Innerhofer-Oberperfler und Breu 2010, 250); (Kesan, Majuca und Yurcik, Cyberinsurance As A Market-Based Solution To The Problem Of CyberSecurity - A Case Study 2005, 16); (Kotulic und Clark 2004); (Kovacs, Markham und Sweeting 2004); (Mello 2013)

[70] (DHS 2013, 18); (ENISA, Incentives and barriers of the cyber Insurance market in Europe 2012, 22); (Friedman, Economic and Policy Framework for Cybersecurity Risks 2011, 11)

and transparent.[71] Since the general idea behind the underwriting process for the insurer is to gauge how likely paying for an event covered by the policy is, underwriters for cyberinsurance policies usually undertake an extensive review of a company. The review is often through a contracted IT security consultant, relying on online questionnaires, on-site audits, previous documentation, and interviews.[72] Companies can convince the insurers that they are taking IT security 'seriously' by adhering to standards and best practices and by explaining their cyber risk management strategies to the insurance company.[73] Through this "rigorous ex ante security assessment," insurance companies hope to get the premium 'right' and mitigate adverse selection and moral hazard.[74]

So, at first glance, it seems that insurance companies have to come up with an underwriting process for cyberinsurance policies. As stated above, the market for cyberinsurance faces many challenges, so why is the status quo of setting premiums an important issue?

First, the premium, the price tag of a policy, is what connects the insurers to the companies buying insurance. As such, the quality of the underwriting process becomes part of the competition between insurers.[75] As the underwriting process is lengthy and complicated, making it expensive for insurance companies. Due to a lack of clarity on cyber risks, insurers are pricing their policies conservatively, i.e. usually at a high price. This discourages many companies from buying cyberinsurance policies.[76] Also, as the underwriting process is not transparent, companies have a hard time comparing different insurers.[77]

Second, premium-setting procedures are not universal and call into question how insurers understand the issue (the cyber world). Do they see cyberinsurance as yet another market or do they take into account special characteristics, e.g. the conceptual challenges outlined above? The conducted nterviews and a growing part of the reviewed literature made it clear that cyberinsurance cannot simply be underwritten as in other markets. However, statements by some insurers and companies show that they have not yet fully realized this challenge. One example is the strategy by several insurance companies "to offer premium discounts to companies that implement certain products or security services […] in hopes of attracting skeptical CIOs". [78]

While this approach is *per se* no problem, it becomes problematic if insurers are relying on the wrong indicators. In more mature insurance markets, such as car insurance, specific characteristics, e.g. the presence of an airbag or anti-lock braking system (ABS), are being rewarded by a lower premium. Following this logic, more than one insurance company offered premium discounts to companies that were using Linux servers instead of another operating systems, based on a statistic that stated that fewer

[71] (Clinton undated, 6); (ENISA, Incentives and barriers of the cyber Insurance market in Europe 2012, 21); (Innerhofer-Oberperfler und Breu 2010, 253, 267)
[72] (Baer und Parkinson 2007, 52f.); (Capgemini 2012, 15); (Clinton undated, 5f.); (Duffy 2002); (Hedrick 2007, 2); (III 2003); (Kesan, Majuca und Yurcik, The Economic Case for Cyberinsurance 2005, 27); (Kesan, Majuca und Yurcik, Cyberinsurance As A Market-Based Solution To The Problem Of CyberSecurity - A Case Study 2005, 11, 13). For an overview of common indicators as well as research for 'good' indicators see (Duffy 2002); (Innerhofer-Oberperfler und Breu 2010)
[73] (ENISA, Incentives and barriers of the cyber Insurance market in Europe 2012, 22)
[74] (ENISA, Incentives and barriers of the cyber Insurance market in Europe 2012, 19); (Kesan, Majuca und Yurcik, Cyberinsurance As A Market-Based Solution To The Problem Of CyberSecurity - A Case Study 2005, 19)
[75] (Innerhofer-Oberperfler und Breu 2010, 252)
[76] (Bandyopadhyay, Mookerjee und Rao 2009, 68); (Herendeen, et al. 2012, 3); (Kesan, Majuca und Yurcik, The Economic Case for Cyberinsurance 2005, 29); (Ponemon, Manaing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age 2013, 4)
[77] (Duffy 2002)
[78] (Gralla 2001)

cyber attacks were measured on Linux servers.[79] There are two problems with this technique: i) the insurers overlooked the fact that Linux, at the time, was not the dominant system, and hence less attractive to attack; and ii) thinking that the equivalent of an airbag or ABS, exists for cyberinsurance. A technology or software alone does not tell us anything about whether a company using it is going to be safer in case of a cyber attack. It is the specific configuration that matters, as one interviewed expert remarked.[80]

Insurers and companies need to better understand the relationship between certain strategies and technologies and the losses incurred due to a cyber attack. While "little has been done to map [normative standards] to the financial losses actually incurred by companies" in the past, this is changing; studies are slowly being undertaken addressing this issue.[81] For example, a recently published Advisen study, found that "organizations who have implemented data breach response plans prior to the breach fare much better than those who have not."[82] Another study by NetDilligence is part of a project that "uses actual cyber liability insurance reported claims to illuminate the real costs of incidents from an insurer's perspective."[83] The study focused on data breach and found, e.g. that there is "no correlation between the number of records lost and the total cost of the breach."[84] Such research is helpful, as it provides insurers with ways of adapting their underwriting process and empowers companies to realize that they might be paying too much for their policies.

If we accept that the underwriting process might not be perfectly informed, a third problem with the status quo emerges. This problem relates to incentives, commonly a perceived benefit of insurers. Price differences for premiums sets the incentive for companies to align themselves with the underwriting standard currently being used. To come back to the example used above, if insurer A is charging companies using Linux servers a lower premium than other companies, *ceteris paribus*, other companies will also switch to Linux servers to save on the premium. What happens, however, if the incentives are based on ill-informed premises? There is historical precedent for such a situation, in the field of IT and in other markets. In the late 1970's fire insurance premiums were mostly determined based on a grading schedule that was not based on research of actual loss data. This had an impact on the local government fire safety planning as the people in charge adapted to the incentives set by the insurance grading schedule only to realize that those incentives were 'wrong' in the sense that they did not lead to lower fire losses.[85] In IT, a similar situation emerged when corporate auditors started demanding firewalls. Companies had to buy firewalls or otherwise be accused of "not following industry best practices […] whether [firewalls] do any actual good or not."[86] Considering the costs of an up-to-date IT security infrastructure, trained personnel and extensive risk-management plans, all incentives set through insurance should be well justified.

Even if one agrees that the status quo of underwriting cyberinsurance is problematic, the question arises: so what? After all, insurance companies have a clear economic interest – "skin in the game" – to get underwriting right. Over time, as their experience grows, the process will get better and better.[87] In

[79] (Gralla 2001); (Kesan, Majuca und Yurcik, The Economic Case for Cyberinsurance 2005, 27) (Kesan, Majuca und Yurcik, Cyberinsurance As A Market-Based Solution To The Problem Of CyberSecurity - A Case Study 2005, 14)
[80] (Toregas and Zahn, Interviews 2013)
[81] (Duffy 2002)
[82] (Advisen 2013, 4); Also see (McKinsey 2013)
[83] (NetDiligence 2013, 1)
[84] (NetDiligence 2013, 9)
[85] (Homer, Lawton und Toregas 1977); (Toregas, Insurance Service Reforms Alter Thrust of Fire Protection - Real Fire History to Affect Insurance Rates 1980)
[86] (Schneier, Hacking the Business Climate for Network Security 2004, 88)
[87] (Baer und Parkinson 2007, 56); (Clinton undated, 5); (A. MacWillson 2012, 2); (Schneier, Hacking the Business Climate for Network Security 2004, 89); (Varian 2000)

response to that argument we raise the question: how long do insurers and companies want to wait? Research and cooperation between the stakeholders focused on the outlined challenges and the setting of premiums in particular can help the cyberinsurance market to achieve its full potential sooner, and overcome the present challenges and inefficiencies.[88]

Suggestions for a research agenda

Cyberinsurance is a welcome and needed addition to the strategies used to deal with the risk of cyber attacks. As in other markets and initial skepticism notwithstanding, cyberinsurance policies are here to stay. However, as the foregoing discussion shows there open questions to what will lead to a more mature cyberinsurance market. The question remains whether one wants to give markets time and accept some initial inefficiencies, or whether one should actively address open issues, be it through research or government action.[89] The goal has to be to move premium modelling away from "art" towards becoming a "science" just as in other markets, to the extent it is possible for cyber risks.[90] This will make sure that cyberinsurance can provide a market-based incentive structure to increase cybersecurity.

First steps in this direction are already being undertaken, see the studies by Advisen and NetDilligence and the work of (Innerhofer-Oberperfler und Breu 2010). This type of research should be extended to cover not only the loss of data, but other risks and costs. Once a better understanding for the quantification of risks and losses exists, research from academia and the private sector should critically assess the processes used by insurance companies when it comes to setting rates. Does it really make sense to give a lower premium to company A, that was classified in a lower risk category according to the research by the insurance company, than to company B in a higher risk category? To this end, insurance companies should make there premium calculation and models even more transparent so that researchers can then check the normative standards against a growing pool of loss data. The risk models used by insurance companies could greatly benefit from such research. Likewise the area offers a great field for interdisciplinary work where academics from computer science and the social sciences can interact to try to answer the question: what is 'good' cybersecurity?[91]
To structure the research agenda, we have grouped some specific questions around the three categories *Policy*, *Management*, and *Technology*. Those categories apply to all the stakeholders, academic researchers, private sector representatives and government officials.

<u>Policy</u>

- Establish a better understanding of CEO attitudes towards cyber risk and preferences towards mitigation strategies by engaging social science, cyber security and finance experts
- Study regional variations in approaches to cyber insurance across the globe and identify common patterns and features
- Investigate differences between insurance and reinsurance regarding national vs. global approaches -> US insurer acts on state level but risk to be insured is global -> is this a problem? Business model has to take this into account

[88] To name but one example, the Atlantic Council is currently engaging in research on correlated risks and its impact for Cyberinsurance.
[89] This paper argues for the former. See (Etzioni 2011) for the case for government involvement.
[90] (Capgemini 2012, 16); (Duffy 2002); (Toregas and Zahn, Interviews 2013)
[91] Stakeholders stated during the Cyber Risk Culture Roundtable that „there's a general lack of objective proof that particular controls – policies, processes, technologies, and otherwise – have measurable and positive risk management impacts" (DHS 2013, 4). See also (ENISA, Incentives and barriers of the cyber Insurance market in Europe 2012, 22). For interdisciplinarity in the study of cyberinsurance see (Böhme und Schwartz, Modeling Cyber-Insurance: Towards A Unifying Framework 2010, 29)

Management

- Explore feasibility of constructing a causal model of cyber threat/response mechanism at enterprise level
- Develop a "big data" strategy linking actual cyber losses and specific variables under the control of management
- Analyze potential of a global cyber loss data base with proper privacy controls and a business model that would make such a data base viable and sustainable

Technology

- Map cyber risk variations for different technology platforms (both in house and Cloud) and provide insights on IT industry perspectives as these platforms change and become more interlinked
- Review Computer Science curricula and identify courses dealing with technology approaches to cyber risk and risk management as an explicit strategy

To broaden the scope of future research in the cyberinsurance market we have also compiled some themes

Food for thought

- Metrics for information security cost (see (Brecht und Nowey 2012, 18ff.); (Innerhofer-Oberperfler und Breu 2010)
- More descriptive surveys to gather more data
- Further investigate the role of different legal frameworks and regulatory regimes
- Further investigate the impact of technologic characteristics, e.g. should the global nature of the Internet change the way we approach risk management? Does the lack of attribution of cyberattacks increase the risk of insurance fraud? How can insurance companies keep up with fast-paced technological innovation
- What private and public initiatives could address cyberinsurance market challenges, e.g. the lack of reinsurance? See TRIA discussion in (Clinton undated, 5); (Homeland Security News

from the literature and our own findings in the category *Food for Thought*.

Interview Outcomes

To complement the literature review, a handful of experts and professionals where ask to provide input. The information they provided is referenced as *Questionnaire*. The small sample of eight people included an insurance lawyer, two insurance companies that offer cyberinsurance policies, a commissioner from the National Association of Insurance Commissioners, a representative at the Insurance Services Office, a representative from a defense contractor, a private sector CISO, and an academic. A snowball-sampling was used starting from an initial sample of publicly available contacts. Given resource constraints, the purpose of the sampling was not to be representative, but to get as many different perspectives on the issue as possible within a reasonable time frame.

Once the sample was identified, data was collected through a questionnaire that was either sent to respondents via e-mail or was used as a basis for an interview (in the case respondents did not want to fill out the questionnaire but still provide insights). The interviews were not transcribed, but answers were noted by the researchers during the interview. All participants consented to being asked and have their answers used for this paper. The questionnaire, which is attached further below, consisted of 12 open-ended questions and a free commentary.

Five out of eight people asked to provide information either returned the filled out questionnaire or agreed to an interview. The respondents include: an insurance lawyer, a commissioner from the National Association of Insurance Commissioners, a representative from a defense contractor, and a private sector CISO and an academic.

Main Findings:

- None of the interviewees thinks that cyberinsurance is just a fad. Instead, all agreed that the market will grow although they differed regarding the speed of growth.
- Awareness of cyber risks varies wildly and while growing, risks are still misunderstood and underestimated.
- Cyberinsurance should play a role in the overall risk management strategy of a company but it should be used in a strategy mix.
- Cyber risks are different from other risks and insurers as well as companies have to take this into account.
- Setting of premiums is still more of an art than a science. Counting on the presence of a given piece of software, the equivalent to an airbag in the car insurance market, is not going to work for cyberinsurance.
- The government should not necessarily intervene to address the challenges the market for cyberinsurance faces today

Questionnaire

1. *Briefly describe the relationship between your employer and insurance against cyber risks, i.e. does your employer buy policies, offer insurance etc.*
   Answer 1:

2. *What does the insurance policy you buy/offer cover? What do you identify as insurable cyber threats and what are uninsurable risks(force majeure)?*
   Answer 2:

3. *Have you ever suffered from a cyber attack? How has it changed your views about insurance against cyber risks?*
   Answer 3:

4. *What role does insurance play in the overall cyber security strategy of your organization? Is it the only protection or is it used in combination with in-house capabilities (e.g. Chief Security Offer (CSO))? Do you consider protection against cyber risk the responsibility of the individual organization or do you see it more as a public good?*
   Answer 4:

5. *What are the reasons driving the decision to purchase insurance? What characteristics are important when comparing different policies/insurance companies?*
   Answer 5:

6. *How do cyber risks differ from other areas of insurance (e.g. car insurance)? Do insurance companies approach it in a similar fashion as other areas of insurance? How do buyers of policies approach it?*
   Answer 6:

7. *How do you set rates for your cyber insurance policies? Actuarial or normative rates (please elaborate)? Do you think your fashion of setting rates is in line with industry practice? Would you support the building of models similar to other, more mature markets (e.g. car insurance)*
   Answer 7:

8. *When looking at the insurance market for cyber risks do you see any problems for the future? Which questions are unanswered at the moment?*
   Answer 8:

9. *Do you think that given the ubiquity of cyber risks, the federal government should take a more active interest in the field, e.g. by providing certification for CSOs or by setting standards for insurance policies?*
   Answer 9:

10. *Do you think, instead of the government, the private sector should more actively engage in initiatives similar to those mentioned in question 9?*
    Answer 10:

11. *How do you judge awareness of cyber risks? Are the risks overestimated or underestimated? What could be done to address misperceptions? Are companies aware of all the options they have to increase cyber security?*
    Answer 11:

12. *Did any of the questions surprise you or got you thinking? Or is knowing the answer to such questions part of your job?*
    Answer 12:

13. *If you feel that there are other relevant aspects to insurance against cyber risks, feel free to mention them.*
    Answer 13:

References

Advisen. "2013 Information Security Cyber Liability \& Risk Management." Tech. rep., Advisen Insurance Intelligence, 2013.

Anderson, Roberta D. "Insurance Coverage for Cyber Attacks - Part One of a Two-Part Article." *The Insurance Coverage Law Bulletin* 12, no. 4 (2013).

Anderson, Roberta D. "Insurance Coverage for Cyber Attacks - Part Two of a Two-Part Article." *The Insurance Coverage Law Bulletin* 12, no. 5 (2013).

Anderson, Ross, et al. "Measuring the Cost of Cybercrime." *WEIS Working Papers.* 2012.

Baer, Walter S., and Andrew Parkinson. "Cyberinsurance in IT Security Management." *IEEE Security \& Privacy* May/June (2007): 50-56.

Bandyopadhyay, Tridib, Vijay S. Mookerjee, and Ram C. Rao. "Why IT Managers Don't Go for Cyber-Insurance Products." *Communications of the ACM* 52, no. 11 (2009): 68-73.

Böhme, Rainer. "Cyber-Insurance Revisited." *WEIS Working Paper.* 2005.

Böhme, Rainer, and Galina Schwartz. "Modeling Cyber-Insurance: Towards A Unifying Framework." *WEIS Working Paper.* 2010.

Brecht, Matthias, and Thomas Nowey. "A Closer Look at Information Security Costs." *WEIS Working Papers.* 2012.

Capgemini. "Using Insurance to Mitigate Cybercrime Risk." Tech. rep., Capgemini, 2012.

Clinton, Larry. "Cyber-Insurance Metrics and Impact on Cyber-Security." *Internet Security Alliance*, undated.

Conti, Gregory, Robert Clark, Chris Rouland, and Jennifer Otterson Mollick. "The Ethics of Hacking Back: Cybersecurity and Active Network Defense." *The Ethics of Hacking Back: Cybersecurity and Active Network Defense.* 2013.

Cordes, Joseph. "An Overview of the Economics of Cybersecurity and Cybersecurity Policy." *CSPRI Report* June (2011): 1-18.

Daniel, Michael. "Incentives to Support Adoption of the Cybersecurity Framework." *Incentives to Support Adoption of the Cybersecurity Framework.* http://www.whitehouse.gov/blog/2013/08/06/incentives-support-adoption-cybersecurity-framework, August 2013.

DHS. "Cyber Risk Culture Roundtable Readout Report." Tech. rep., National Protection and Programs Directorate Department of Homeland Security, 2013.

Duffy, Daintry. "Cybersecurity Insurance: Safety at a Premium." *Cybersecurity Insurance: Safety at a Premium.* http://www.cio.com/article/217739/Cybersecurity_Insurance_Safety_at_a_Premium, December 2002.

Elliott, Tim, and Yemi Saka. "Rebuilding confidence in financial services through robust cyber security strategies." *Accenture*, 2010: 1-20.

ENISA. "Incentives and barriers of the cyber Insurance market in Europe." Tech. rep., European Network and Information Security Agency, 2012.

ENISA. "Introduction to return on Security Investment - Helping CERTs assessing the cost of (lack of) security." Tech. rep., ENISA, 2012.

Etzioni, Amitai. "Cybersecurity in the Private Sector." *Issues in Science and Technology* Fall (2011): 58-62.

Foster, Andrea L. "Worried About Hackers? Buy Some Insurance." *The Chronicle of Higher Education* October (2006).

Friedman, Allan. "Cyber Theft of Competitive Data: Asking the Right Questions." *Center for Technology Innovation at Brookings* September (2013): 1-7.

Friedman, Allan. "Economic and Policy Framework for Cybersecurity Risks." *Center for Technology Innovation at Brookings* July (2011): 1-24.

Gordon, L. A., and M. P. Loeb. "The Economics of Information Security Investment." *ACM Transactions on Information and System Security* November (2002).

Gordon, Lawrence A., Martin P. Loeb, and Tashfeen Sohail. "A Framework for Using Insurance for Cyber-Risk Management." *Communications of the ACM* 46, no. 3 (2003): 81-85.

Gralla, Preston. "Insurance for Online Attacks Has Yet to Catch On." *Insurance for Online Attacks Has Yet to Catch On.* December 2001.

HBR. "Meeting the Cyber Risk Challenge." Tech. rep., Harvard Business Review Analytic Services, 2013.

Hedrick, Alison. "Cyberinsurance: A Risk Management Tool?" *Information Security Curriculum Development Conference.* 2007.

Herendeen, Tom, Mark Greisinger, Bob Parisi, and John Mullen. "Cyber Liability The Sequel: One Year Later, What's Changed?" *Cyber Liability The Sequel: One Year Later, What's Changed?* http://www.bestreview.com/webinars/cyber12/transcript.pdf, February 2012.

Homeland Security News Wire. "Terrorism insurance should cover cyberterrorism." *Terrorism insurance should cover cyberterrorism.* http://www.homelandsecuritynewswire.com/dr20131024-terrorism-insurance-should-cover-cyberterrorism-industry, October 2013.

Homer, Porter W., John W. Lawton, and Costis Toregas. "Challenging the ISO Fire Rating System." *Public Management* July (1977): 2-6.

III. "Most Companies Have Cyber-Risk Gaps in Their Insurance Coverage, States the I.I.I. - Traditional Insurance Policies Not Adequate For Cyber Exposure." *Most Companies Have Cyber-Risk Gaps in Their Insurance Coverage, States the I.I.I. - Traditional Insurance Policies Not Adequate For Cyber Exposure.* http://www.iii.org/media/updates/archive/press.731722/index.html, August 2003.

Innerhofer-Oberperfler, Frank, and Ruth Breu. "Potential Rating Indicators for Cyberinsurance: An Exploratory Qualitative Study." Chap. 13 in *Economics of Information Security and Privacy*, edited by Tyler Moore, David J. Pym and Christos Ioannidis, 249-278. Springer, 2010.

ISO. *ISO introduces cyber risk program to help cover $7 trillion e-Commerce market.* January 2005. http://www.iso.com/Press-Releases/2005/ISO-INTRODUCES-CYBER-RISK-PROGRAM-TO-HELP-COVER-$7-TRILLION-E-COMMERCE-MARKET.html.

ITRC. "Breach Report." Tech. rep., Identity Theft Resource Center, http://www.idtheftcenter.org/ITRC-Surveys-Studies/2012-data-breaches.html, 2012.

Kesan, Jay P., Ruperto P. Majuca, and William J. Yurcik. "Cyberinsurance As A Market-Based Solution To The Problem Of CyberSecurity - A Case Study." *WEIS Working Paper*. 2005.

Kesan, Jay P., Ruperto P. Majuca, and William J. Yurcik. "The Economic Case for Cyberinsurance." Tech. rep., Illinois Law and Economics Working Papers Series No. LE04-004, 2005.

Kobayashi, Bruce H. "An Economic Analysis of the Private and Social Costs of the Provision of Cybersecurity and other Public Security Goods." *Supreme Court Economic Review* 14 (2006): 261-280.

Kotulic, Andrew G., and Jan Guynes Clark. "Why there aren't more Information Security Research Studies." *Information \& Management* 41, no. 5 (2004): 567-607.

Kovacs, Paul, Melissa Markham, and Robert Sweeting. "Cyber-Incident Risk in Canada and the Role of Insurance." Tech. rep., Institute for Catastrophic Loss Reduction, 2004.

MacWillson, Alastair. "Plugging the Hole: Cyber Security in Insurance Podcast Transcript." *Accenture*, 2012: 1-3.

MacWillson, Alistair, Bill Phelps, Floris van den Dool, and Paul O'Rourke. "Traditional apapproach to information security are no longer sufficient." *Accenture Technology Reports*, 2011: 1-36.

McKinsey. "How good is your cyberincident-response plan?" *How good is your cyberincident-response plan?* http://www.mckinsey.com/Insights/Business_Technology/How_good_is_your_cyberincident_response_plan!, December 2013.

Mello, John P. "Rise in data breaches drives interest in cyber Insurance." *Rise in data breaches drives interest in cyber Insurance.* http://www.csoonline.com/article/738140/rise-in-data-breaches-drives-interest-in-cyber-insurance, August 2013.

NetDiligence. "Cyber Liability \& Data Breach Insurance Claims." Tech. rep., NetDiligence, 2013.

Nordman, Eric. "Managing Cyber Risks." *CIPR Newsletter* October (2012): 28-29.

Pasciullo, Nicholas A. "Insurance and High Technology: Consistency In Claims And Coverage Resolution." *Insurance and High Technology: Consistency In Claims And Coverage Resolution.* http://corporate.findlaw.com/law-library/insurance-and-high-technology-cyberinsurance-consistency-in.html, March 2008.

Phelps, Bill, Floris van den Dool, and Paul O'Rourke. "A More Effective, Simple and Cost Efficient Approach to Protecting Critical Enterprise Data." *Accenture High Performance IT Insights*, 2012: 1-12.

Ponemon. "2013 Cost of Data Breach Study: Global Analysis." Tech. rep., Ponemon Institute, 2013.

Ponemon. "Manaing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age." Tech. rep., Ponemon Institute LLC, 2013.

PRNewswire. "Cyber Monday Attacks Cost Organizations up to $3.4 Million per Hour in Losses, RSA Finds." *Cyber Monday Attacks Cost Organizations up to $3.4 Million per Hour in Losses, RSA Finds.* http://www.marketwatch.com/story/cyber-monday-attacks-cost-organizations-up-to-34-million-per-hour-in-losses-rsa-finds-2013-10-28, October 2013.

Ryan, Julie. "Cyber Security: The Mess We're In and Why It's Going to Get Worse." *CSPRI Report* April (2011): 1-13.

Santo, John Del, Andy Starrs, and Emmanuel Viale. "Accenture Technology Vision 2013: Every Insurer is a Digital Insurer." *Accenture Insurance Report*, 2013: 1-20.

Schneier, Bruce. "Hacking the Business Climate for Network Security." *IEEE Computer* April (2004): 87-89.

Schneier, Bruce. "Hacking the Business Climate for Network Security." *IEEE Computer* April (2004): 87-89.

—. "Security ROI: Fact or Fiction?" *Security ROI: Fact or Fiction?* http://www.csoonline.com/article/446866/security-roi-fact-or-fiction-, September 2008.

Toregas, Costis. "Insurance Service Reforms Alter Thrust of Fire Protection - Real Fire History to Affect Insurance Rates." *County News* January, no. 14 (1980): 5-8.

Toregas, Costis, and Nicolas Zahn. "Interviews." 2013.

Varian, Hal R. "Managing Online Security Risks." *Managing Online Security Risks.* June 2000.

Wheeler, John. "Security Think Tank: When cyber insurance is right and when it is not." *Security Think Tank: When cyber insurance is right and when it is not.* http://www.computerweekly.com/opinion/Security-Think-Tank-When-cyber-insurance-is-right-and-when-it-is-not, October 2013.

Wood, Lamont. "Can 'cyberinsurance' protect you from data breach catastrophe?" *Can 'cyberinsurance' protect you from data breach catastrophe?* June 2007.