Cyber and Reputational Risk Insurance

Past, Present, and Future

By

Justin Litaker

Appalachian State University

Risk Management & Insurance and Marketing Double Major

Cyber and Reputational Risk Insurance
Past, Present, and Future

Table of Contents

Introduction

In today's society it is virtually impossible for a business to be successful without the incorporation of the Internet. Most companies today have a presence on the web consisting of at least a company webpage. Some have gone even further: creating their own social networking pages, online commercials, blogs, wiki's, and apps. With this new age of technology a greater level of efficiency can be achieved, but with this increased level of efficiency comes the risk of a growing number of exposures. A number of these new exposures are excluded by the Commercial General Liability (CGL) coverage and other standard policies. Creating a dilemma for businesses because their success is dependent upon their ability to reach their consumers and consumers today use the Internet more frequently than ever before for pre-purchase information and purchasing goods. These exclusions paired with businesses desires to be protected while operating on the web have brought rise to both the cyber risk and reputational risk insurance products.

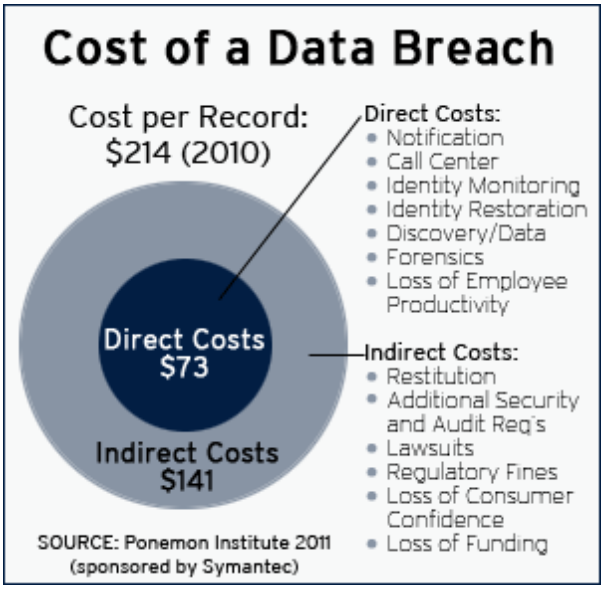
This paper will first analyze the exposures businesses are currently facing and how these exposures have lead to the creation and development of the cyber risk product. Since the creation of the cyber risk product, new exposures have created a need for another new insurance coverage; an insurance coverage that will help an organization repair its reputation after it has been tarnished or diminished. A few insurers in the property and casualty market have responded to this need by releasing a new insurance product that is being referred to as, reputational risk insurance. This paper will analyze how the needs of businesses have driven the

creation of the cyber and reputational insurance products and where these businesses are driving the need for insurance products in the future.

Exposures Businesses Face in Cyberspace

Companies are expanding beyond their brick and mortar locations through the help of the Internet. The Internet allows users to access a number of different sites and is sometimes referred to as cyberspace, which is "the online world of computer networks that has facilitated communication, accelerated the transmission of data, and revolutionized the way the world works" (Schirick). Through cyberspace businesses can create their own websites, blogs, apps, and social media sites. All of these options have been made available by the Internet and have significantly enhanced businesses marketing capabilities. With the use of the Internet a company can more easily reach their target segment, make more frequent contacts with their segment, and work on building relationships with their segment. From a marketing standpoint the Internet can be a great resource that could allow a company to achieve increased efficiency and effectiveness. For this reason, businesses have jumped into the world of cyberspace with both feet, but few have stopped to consider the possible risks associated with this decision. When evaluating the potential risks associated with the use of the Internet there are two major risks that businesses are becoming more and more aware of and they are the cyber risk of a data breach and the reputational risk of a company losing potential business because its character or quality have been called into question.

A data breach can be a serious incident for a business and could cost an enormous sum of money to handle. The average cost of a data breach in 2010 was $214 per lost record. This may seem like an insignificant amount of money at first glance but when it is taken into consideration that most companies who suffer a data breach will lose hundreds, thousands, or even millions of records, depending on the size of the company, the average cost of a data breach can become expensive in a very short amount of time. According to a recent study by the Insurance Information Institute, "the average organizational cost of a data breach is $7.2 million" (Fox & McGinley). Some of the costs that are taken into consideration when determining the average cost of a data breach include the "cost of detection, escalation, notification and response. Then consider the legal, investigative, administrative and reparation expenses. These are then compounded by potential customer defections, opportunity loss, reputation management and reduction in shareholder value" (Fox &McGinley). Below is visual found on Willis' website that breaks down the cost per record in direct and indirect costs associated with a data breach (Magrann-Wells).



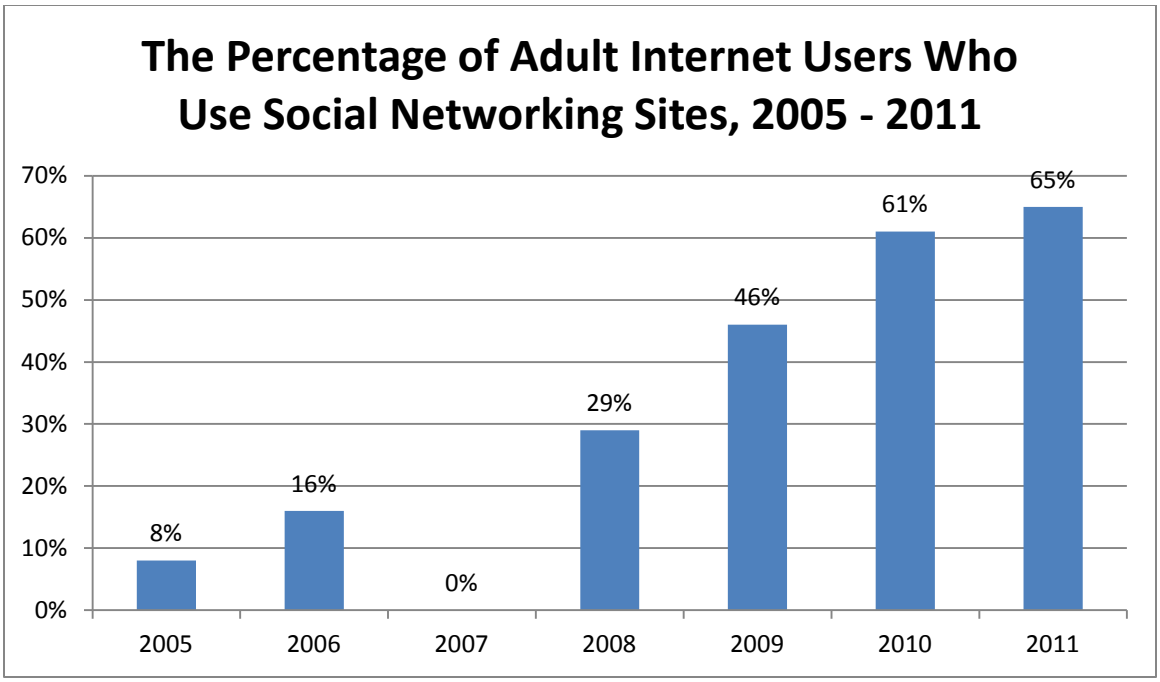
Reasons for Increasing Demand in the Future

A data breach can be a very serious matter for an organization and is defined as "an incident (or series of incidents) in which sensitive, protected or confidential information has been potentially viewed, stolen or used by an individual or entity unauthorized to do so" (Fox & McGinley). There have been an increasing number of data breaches and cyber attacks over the past few years. For this reason businesses will be looking to buy protection for this exposure, which will in turn increase the demand for cyber risk products in the future. Increased demand can be a good thing but with the size of the average loss associated with cyber losses begin so great, insurers will have to be attentive to the principle of adverse selection. It is possible that the businesses looking to buy this product might be choosing this option over properly protecting their information. This is where stringent underwriting will be critical for the success of this product as demand increases.

An even newer product that has been recently introduced to the property and causality market is the reputational risk insurance product. At this time there are only a few insurers who have developed these types of policies. Essentially the reputational risk policy has been developed to insure the loss created by a reputational attack or threat made to an organization that results in a loss in reputation. Reputational risk is associated with indirect costs and could be an important coverage to couple with the cyber risk product because many reputational losses can arise out a cyber attack.

The emergence of the reputational risk product has coincided with the increased popularity of social media. Businesses recognize that their consumers access these sites on a

regular basis and realize to best reach their customers they too will need to create a presence on social media sites. The problem with this is that social media sites allow for interactivity between users (individuals and businesses) which leaves a business open to the risk of a individual or entity posting damaging information on a social media site about the business. To repair their image the business will then have to respond to this damaging information, which can be costly. It can be costly because the business will want to restore its image and reputation to the state it was at prior to the damaging information coming out. To accomplish this it will take more than one refuting press release. For this reason, Aon along with Zurich, Kiln along with Willis, and Chartis have all released reputational risk policies to respond to the needs of businesses based on the current business environment. The term reputational risk refers to "a company's risk of having its reputation damaged because of certain events or incidents and the fallout that takes place because of these incidents" (O'Connor). A few insurers up to this point have been willing to insure this type of risk, if the product can be profitable for the insurer while maintaining an equitable price for the consumer this coverage could potentially be the next big thing in the insurance industry. Below is a chart from the Insurance Information Institute study depicting the increase in adults over the age of thirty using social media from 2005 to 2011 (Hartwig).



*2007 data not available

Cyber and Reputational Losses in 2011

Data breaches not only result in direct losses, but also include indirect losses in the form of a reputational loss. A reputational loss is characterized by an event or incident that ultimately damages the reputation of a company's brand image or product. In some cases, the effects of a reputational loss can be severe enough to put a company out of business (O'Connor). Examples of these types of losses are becoming more common, with an increasing number of losses over the past few years. Some of the largest and more well known data breaches from the year 2011 include: Sony Corp's online game networks, (then just months later) Sony Playstation's network, WordPress (an online blog social networking site), University of South Carolina, University of Connecticut, TripAdvisor (a subsidiary of Expedia), and Call of

Duty Black Ops (Fahmida). These are all organizations, products, institutions, or companies that most consumers are familiar with and all of them suffered from cyber attacks in 2011.

The Sony example of having two breaches in a six month span is extreme. Between the two data breaches a rough estimate of almost two hundred million accounts were compromised. The first cyber attack of Sony compromised over one hundred million accounts in April 2011 and the second attack on Sony compromised ninety three million user accounts in October 2011 (Hartwig). With these two cyber attacks, hackers collected Sony users: "names, emails, addresses, login credentials, and credit card information" (Fahmida). The hackers were able to access Sony's data by attacking the three cloud system Sony was using to store its customers information. It is likely Sony will face both reputational losses as well as cyber losses through litigation from users whose information was accessed by cyber criminals through Sony's insecure cloud database system.

Another example of a cyber attack occurred on April 14th 2011. The target was an online blogging and social media site known as WordPress. WordPress experienced a distributed denial of service attack (DDoS), which is a unique type of cyber attack that knocks the site offline for a period of time (Wagenseil). This type of attack exposed only the passwords of users; because the cyber attack was aimed at taking WordPress offline for a period of time it is likely that the major concern for WordPress at this point is a reputational loss. This attack showed users of WordPress that the site is vulnerable to hackers, likely shaking the faith users once had in the site prior to the attack. This type of reputational loss is one that may lead to

users of the site deactivating their accounts and switching to another social media blogging site where the perceived level of security is greater.

Two Big Areas of Exposure

As the two previous examples show, businesses need to be aware of the risks they are exposing themselves to when deciding to create their presence on the Internet. In today's competitive and global business environment companies cannot afford to forego the opportunity that the Internet has to offer. Many companies will maintain their own website where products or services can be quickly and readily purchased, companies create their sites in this way because it allows for customers to buy directly from the web, which can boost sales with little to no additional cost on the part of the retailer. This can be a great bottom line booster for companies but it can also be a large liability exposure too. These types of sites collect all kinds of personal information at the time of purchase, making them a desirable target for a cyber criminal looking to commit identity theft. Following the cyber attack the company's reputation could also be ruined. This is just another example of when a cyber exposure could develop into both a cyber and reputational loss.

The second potential online exposure that many companies are choosing to participate in is social media and blogging. These sites are unique in that they are centered on the idea of creating an interactive environment on the web where users can send text, picture, and video based messages to one another. One of the largest liabilities associated with social media and blogs is that a company cannot control what another user publishes on these types of sites,

creating an enormous reputational exposure for businesses. A user of a given social media or blog site could publish damaging information about a company; which in turn could hurt the company's image and reputation with its customer base. For this reason, it is necessary that with this type of exposure, organizations develop a crisis management plan. It is important that this plan has already been developed and is in place well before an occurrence or reputational attack occurs. Once a crisis management plan has been put together, the company should consider how they plan to finance the execution of the plan. Two options for financing the crisis management exposure are through an insurance policy (reputational risk policy) or a retention fund. Basically, handling the reputational risk from the businesses perspective is a two step process, first it is important to have a crisis management plan in place to handle these issues as quickly and effectively as possible, but even the most well thought out crisis management plan is worthless without the proper financing for executing the crisis management plan.

Cyber Risk Policies

Cyber risk insurance policies have been offered by insurers for the past couple years and have recently been developed into modular packages. The idea behind designing the cyber risk product into a modular package is that it allows the insured to purchase a pre-developed comprehensive package of coverages, but if one would prefer to select certain coverages for purchase individually, that option is still made available. One example of an insurance company that is offering their cyber risk product in a modular package is Chartis. Chartis has their own modular cyber risk package called the Specialty Risk Protector. The Specialty Risk Protector is

described in an August 2010 press release as the “market leading professional liability and data networking security insurance solution developed […] to give customers access to additional protection for critical networking security and privacy risks, greater flexibility in managing data breach events, and new tools to prevent losses” (Press Release). The three policies currently offered under Chartis’ Specialty Risk Protector package are: security and privacy liability insurance, cyber extortion insurance, and network interruption insurance. For the purpose of this paper, the Chartis policies will be used for examining the cyber risk insurance coverage. Many other excess and surplus lines insurers offer similar packages and coverages.

The first coverage mentioned in the Specialty Risk Protector package is the security and privacy liability insurance coverage. The security and privacy liability insurance policy is coverage for a claim alleging a security failure or privacy event. A “security failure” or “privacy event” could potentially include three different types of loss as they are defined within the policy: 1) a failure or violation of the security of a computer system including, unauthorized access, unauthorized use, denial of service attack, or transmission of malicious code; 2) physical theft of hardware controlled by the company on which electronic data is stored, by someone other than an insured, from a premises occupied by and controlled by the company; 3) failure to disclose an event which may result in an identity theft of an individual or corporation. Essentially this coverage is a claims made third party coverage. Meaning that for there to be coverage an insured must first be sued in relation to a security failure or privacy event. Once this situation arises, the insurer would then provide defense costs to the insureds and pay the claim based on an evaluation of the coverage triggers and exclusions as they relate to the claim made against the insured.

This type of coverage would have been beneficial for Sony to have had in the previous example where they suffered two data breaches compromising millions of their customer's records. With the information gained by the data breach it would be very easy for the cyber criminals who breached Sony's data to steal the identity of all the compromised accounts, and incur all kinds of debt under the assumed identities. In this scenario, the consumers who are victims of this act of identity theft would then sue Sony for the debt incurred by the identity theft. If Sony purchased the security and privacy liability product they would probably receive the costs of their defense, if not the entire claim, after the retention limit (deductible) had been sufficiently meet.

The second coverage offered by the Specialty Risk Protector is cyber extortion insurance. Unlike the privacy and security coverage, the cyber extortion coverage is an occurrence based first party coverage. The insuring agreement for this policy states that the insurer will pay losses an insured incurs as a result of a "security threat." A security threat is defined in the policy as "any threat or connected series of threats to commit an intentional act against a computer system for the purpose of demanding money, securities or other tangible or intangible property of value from an insured" (Policy Number 101017). As the name of the coverage insinuates, the cyber extortion policy is coverage for an attack on a company's computer system by an individual who is seeking payment in the form of money, securities, or some other form of tangible property in exchange for not publishing or exposing the compromised information.

The cyber extortion coverage fits very well with reputational risk product that has just recently been released to the consumers over the last few months. In the case of a cyber extortion attempt on a company, it is likely that if the extortion attempt is mishandled by the insured and insurer that the compromised information would then be published for everyone to see and in turn create a reputational threat to the business. For this reason, it is foreseeable that the cyber extortion product and the reputational risk product may be bundled together in the future to provide a more comprehensive product. Another reason the products may want to be bundled together in the future has do with the ethical dilemma that could be created when there are two insurers, one handling the cyber extortion policy and a second handling the reputational risk policy. In this scenario it is plausible that when an extortion attempt occurs and the compromised information is published hurting the reputation of the insured business, that both companies will point the finger at one another claiming it is excluded from their policies but insured under the others. This situation could be alleviated by, providing both the cyber extortion policy and the reputational risk policy together, in a package, through the same insurance company. By providing the two coverages in a package the complications in determining which insurer is liable for an extortion and then reputational loss would be lessened.

The third coverage provided by the Specialty Risk Protector package is the network interruption insurance policy. This coverage, much like the cyber extortion policy, is an occurrence based first party coverage. The insuring agreement states the insurer will pay losses that an insured incurs after the waiting hours period (a set number of hours stated in the declarations) and solely as a result of a security failure. It is important to note that a security

failure is defined differently in this policy from the way it was previously defined in the privacy and security policy. In this policy a “security failure” is defined as a failure or violation of the security of a computerized system, which includes any unauthorized access, unauthorized use, denial of service attack, or transmission of malicious code and also includes any failure or violation resulting in theft of a password from a company’s premises, computer system, or an officer, director, or employee of a company by non-electronic means in direct violation of a company’s specific written security policies. The coverage appears to provide a partial overlap in protection with the privacy and security policy by providing coverage for the violation of a computerized system and the unauthorized access, use, denial of service attack, or transmission of malicious code. The network interruption coverage then takes the security and privacy policy a step further by also providing coverage for the physical theft of a password or access code.

Over the past few years cyber risk insurance has become a well rounded and developed product. For this reason, the cyber risk insurance product is probably fairly well cemented within insurance companies as it is currently packaged and written, but as the demand for the cyber risk insurance increases in the future, insurers will need to provide tools to help their insureds better protect themselves from cyber criminals. By doing this the insurance companies will also be protecting themselves from a high number of expensive claims. Some insurance companies have already begun to look at this aspect of service, “Chubb says it will reimburse its cyber liability insurance customers, where permitted, as much as one-half the cost of products from AirPatrol Corporation that are designed to prevent mobile devices from exposure to cyber attack” (Speer). Even though Chubb has not invested in the technology themselves, they have

outsourced and incentivized their insureds ability to receive cyber security protection services. In the future cyber risk insurance will be bought primarily for the service the insurance company provides in helping a business secure its cyber risk exposures. Another reason insurance companies should look into helping purchasers of cyber risk insurance with their risk management of cyber risk exposures is that the average loss suffered by a business who experiences a cyber attack, where data is breached, is $7.2 million. The insurance companies cannot afford to pay a number of these claims while keeping rates adequate and desirable. For this reason, insurance companies will need to either invest in the technology necessary to help protect their insureds from cyber risk or outsource this function to someone else, like Chubb has begun to experiment with. By doing this, the insurance company will be helping their insureds secure their online exposures, which will provide the insured with a superior cyber protection service and the insurer with a more secure risk.

Reputational Risk Policy

Reputational risk has been around for a long time, and is the "risk that a company will lose potential business because its character or quality has been called into question" (Reputation Risk). It has been within the last six months that insurance carriers have begun to insure this type risk. The following is a press release from Chartis that was published on October 11th 2011: "The Chartis insurers today, introduced ReputationGuard, an insurance policy that provides innovative coverage to help policyholders cope with reputational threats. Developed by Chartis' Executive Liability division, ReputationGuard delivers the benefit of both access to

world-class reputation and crisis communications professionals as well as coverage for costs associated with avoiding or minimizing the potential impact of negative publicity" (Ali). With this insurance coverage being so new, only a few insurers are currently offering it. For the purpose of analysis, this paper will be looking at Chartis' ReputationGuard product. A few other insurers have their own reputational risk insurance product at this point, but the products are not very similar. For example, Kiln along with "Willis, [one of the other insurers and brokers offering reputational risk insurance product,] are taking a more segment specific route with their new Hotel Reputation Protection 2.0 policy, which responds to incidents that lead to, or are likely to lead to, hotel business losses from adverse publicity through any medium, from traditional to new media" (O'Connor). Kiln is taking a much more segmented approach to insuring reputational risk, while Chartis on the other hand is offering a reputational insurance coverage that is geared to insure just about any type of business.

Chartis' ReputationGuard product has two coverage triggers, the first is a reputation threat mitigation coverage which states that the insurer will pay the proactive costs that an insured incurs in seeking to avoid or minimize the potential impact of a specific reputation threat. With this first coverage trigger, it is important to identify what is included within the term proactive costs and what the definitions the terms Panel PR Firm and reputation threat are. Proactive costs are the consultation costs associated with the crisis communication services provided by a Panel PR Firm, incurred by an insured in connection with a reputation threat before a reputation attack occurs. A Panel PR Firm is any public relations, crisis management, or brand management firm specifically retained by the insured in connection with a reputational threat or attack. Reputation threat is defined as any act or event that the named entity believes

would if disclosed in publication, be seen by any insured's stakeholders as a material breach of trust and have an adverse impact on the public perception of an insured or covered brand.

The second coverage trigger deals with reputation attack response coverage. This is coverage for the response costs (consultation costs and targeted communications costs designed to address a reputation attack) that an insured incurs in attempting to minimize the potential impact of a "reputation attack." A reputation attack is any publication by a third party that the named entity believes will be seen by any of the insured's stakeholders as a material breach of trust that is likely to have an adverse impact on the public perception of an insured or covered brand. Essentially the first coverage trigger mentioned, is covering the threat of a reputational attack, while the second coverage trigger is going to provide coverage for when the third party goes forth with a reputational threat, publishing the damaging material and creating a reputational loss. One important thing to note about this coverage is that for there to be coverage, the policy requires that an insured hire a Panel PR Firm from a list preselected by Chartis. Currently, there are only two Panel PR Firm options allowed by Chartis and they are Burson-Marsteller and Porter Novelli. Both firms are large international Panel PR Firms who specialize in a range of clients including: corporate, healthcare, technology, and consumer communications (Burson & Porter).

With the ReputationGuard product Chartis is "most interested in [businesses] with revenues of $500,000 to $2 billion" (O'Connor). The reasoning behind this decision according to Robert Yellen, the chief underwriting officer for the executive liability division of Chartis in New York is, "the product is targeted to middle-market companies because larger companies are

more likely to have in-house teams to deal with these issues" (O'Connor). The logic behind this decision makes sense, especially with this being a new product; insurance companies are not looking to insure the reputation of an Apple, Inc. The magnitude of a loss with a company of that size would be too large for any insurance carrier to be comfortable experimenting with a new insurance product. Deciding to test this product with the middle market segment allows the insurance companies to determine their tolerance level for reputational risk without leveraging too much if a significant number of losses do occur. For the first few years this product could be very profitable for the few insurers currently offering reputational risk coverage. Reputation risk has been stated as the number one or two concern in regards to exposures they're currently facing, for this reason the product should be a desirable coverage. Once the few major players involved in issuing reputational risk products begin to reap the rewards of being first to the market with their product, other carriers will compile their own reputational risk product in an attempt to get a piece of the pie. As competition increases, often underwriting standards loosen and this is where many companies could become over leveraged. Reputational risk is a large exposure to insure, while the claims may have a low frequency in occurrences, the dollar amount associated with each claim can be astronomical. For this reason two to three years from now when competition peaks in the industry among insurers offering this product, carriers need to remember that they are staking their reputation on the reputations of others by insuring reputational risk when underwriting this product.

Conclusion

With the perils of the Internet increasing on an almost daily basis it is important that the insurance industry listen to the needs and concerns of their P&C clients. Over the past few years it is evident through the rise of the cyber risk and reputational risk insurance coverages that the insurance industry is attempting to meet the needs of its consumers as they arise. At this point, the big question is, whether reputational risk insurance is a sustainable product. If so, it truly could be the next big thing in insurance. Only time will tell if this product truly is and can be a sustainable, profitable product for the industry. If the losses aren't too large within the first couple years, all the other carriers will jump on board and offer reputational risk coverage too, but there will be losses and with a reputation loss, there is a strong chance that at some point there will be a catastrophic loss. So, while companies are collecting the profits associated with this product's success, they should probably store a significant portion of that profit away as excess for when the catastrophic reputational loss strikes.

Work Cited

Ali, Marie. "Chartis Launches ReputainGuard, Reptuational Risk Insurance." *Business Wire*. Chartis, 11 October 2011. Web. 13 Feb 2012. <http://www.businesswire.com/news/home/20111011006194/en/Chartis-Launches-ReputationGuard®-Reputational-Risk-Insurance>.

Brew, Oliver. "Liberty International Underwriters VP Says Cyber Liability Writers Seeing Increase in Insured Claims." *Best*. Interview. 08 February 2012. Print.

Burson-Marsteller, n.d. Web. 13 Feb 2012. <http://www.burson-marsteller.com/ default .asp&xgt;.

Fahmida, Rashid. "IT Security & Network Security News & Reviews: 10 Biggest Data Breaches of 2011 So Far." *eWeek.com*. N.p., 25 May 2011. Web. 12 Feb 2012. <http://www.eweek .com/c/a/Security/10-Biggest-Data-Breaches-of-2011-So-Far-175567/>.

Fox, Carol and McGinley, Brian. "ERM Best Practices In The Cyber World." *RIMS Executive Report*. RIMS, n.d. Web. 11 Feb 2012.

Gaynor, Anna. "Liberty National Underwriters Offers New Cyber Liability Coverages." *Business Insurance*. N.p., 09 February 2012. Web. 11 Feb 2012.

Hartwig, Robert. "Social Media, Liability And Insurance." *Insurance Information Institute*. N.p., December 2011. Web. 11 Feb 2012.

Kiln. N.p., n.d. Web. 27 Feb 2012. <http://www.kilngroup.com/>.

Lee, Danielle. "PwC Reports Increase In Fraud, Cyber Crime." *Insurance Networking News*. N.p., 01 December 2011. Web. 11 Feb 2012.

Magrann-Wells, Richard. "Scariest Financial Services Risk: Data Breach." *WillisWire*. 31 Oct. 2011. Web. 20 Feb. 2012. <http://blog.willis.com/2011/10/scariest-financial-services-risk-data-breach/>.

O'Connor, Amy. "The Next Big Thing In Insurance Coverage Is Here." *Insurance Journal*. N.p., 13 December 2011. Web. 11 Feb 2012. <http://www.insurancejournal.com/news/national/2011/12/13/226947.html>.

Porter Novelli, n.d. Web. 13 Feb 2012. <http://www.porternovelli.com/>.

Press Release, . "Chartis Enhances Specialty Risk Protector To Address Evloving Privacy And Data Security Risks." *Chartis*. N.p., 18 August 2010. Web. 11 Feb 2012.

Quinley, Kevin. "Managing Social Media Risk." *IRMI*. N.p., 07 March 2010. Web. 11 Feb 2012.

"Reputation Risk." *BusinessDictionary.com*. N.p., n.d. Web. 13 Feb 2012. <http://www.businessdictionary.com/definition/reputation-risk.html>.

Schirick, Edward. "Risk Management: Cyberspace - Risks In A Networked World." *American Camp Association*. N.p., August 2006. Web. 11 Feb 2012.

"Social Media's Big Business Risks." *Insurance Networking News*. N.p., 25 October 2011. Web. 11 Feb 2012.

Speer, Pat. "Chubb Offers Cyber Liability Incentives." *Insurance Networking News*. N.p., 27 October 2011. Web. 11 Feb 2012.

Wagenseil, Paul. "WordPress.com Data Breach Puts Millions Of Bloggers At Risk." *MSNBC.com*. N.p., 14 April 2011. Web. 12 Feb 2012. <http://www.msnbc.msn.com /id/42596276 /ns/technology_and_science-security/t/wordpresscom-data-breach-puts-millions-bloggers-risk/