FDCC
QUARTERLY
VOL. 63, NO. 3 SPRING, 2013

FEDERATION OF DEFENSE & CORPORATE COUNSEL

FDCC QUARTERLY

SPRING, 2013 VOLUME 63, NUMBER 3

CONTENTS

Cite as: 63 FED'N DEF. & CORP. COUNS. Q. ___ (2013).

The Federation of Defense & Corporate Counsel Quarterly is published quarterly by the Federation of Defense & Corporate Counsel, Inc., 11812 North 56th Street, Tampa, FL 33617.

The Emperor's New Clothes and Cyber Insurance

A Few Questions Go a Long Way When Evaluating the "Bare" Essentials of a New Product Amidst a New and Dangerous Risk

Michael T. Glascott
Aaron J. Aisen

I.
Illusions About Cyber Risks, Cyber Security, and Cyber Insurance Coverage: The Parallel to *The Emperor's New Clothes*

The Danish storyteller Hans Christian Andersen told the story of a vain and foolish emperor duped by an illusion.[1] Two tailors came to town and offered to make the emperor a set of clothes of the finest quality; however, the tailors told the emperor, the clothes were invisible and could only be seen by the wise. The emperor liked the idea of being able to distinguish which of his subjects were wise, so he instructed the tailors to make the clothes. At first, the emperor felt awkward about the invisible suit, but not wanting to appear foolish, he claimed he could see the clothes and, for the same reason, so did his wife and his servants. Each wanted to avoid appearing foolish.[2]

The emperor wore his new clothes on parade before his subjects and, having heard that only the wise could see the clothes, all of them pretended to see the clothes. The illusion created by the tailors continued until a young boy, unaware of the need to appear wise, cried out that the king was naked. And so, the willingness to embrace an illusion resulted in embarrassment to the king and his subjects.[3]

---

[1] Hans Christian Andersen, *The Emperor's* New *Clothes*, Project Gutenberg's Andersen's Fairy Tales (last updated Jan. 26, 2013), http://www.gutenberg.org/files/1597/1597-h/1597-h.htm#link2H_4_0001.

[2] *Id.*

[3] *Id.*

Michael T. Glascott is a partner in the Global Insurance Services Practice Group of the Buffalo, N.Y. office of Goldberg Segalla LLP. Mr. Glascott counsels clients and litigates matters involving insurance coverage, bad faith and commercial issues as well as personal injury defense. Mr. Glascott has successfully represented insurer clients in courts throughout New York and other northeastern states such as Ohio, New Jersey and Delaware. He is a former Assistant District Attorney and has successfully litigated matters while engaged by private law firms in Tulsa, Oklahoma, and Buffalo, New York. Mr. Glascott currently serves the Federation of Defense & Corporate Counsel as a member of the Board of Directors and Eastern Coordinator for State Representatives. He is also a member of several committees including the Financial Review Committee, Admissions Committee and is a past chair of the Insurance Coverage Section.

As society has become more reliant on technology when conducting business, the amount of personal and proprietary information that third parties possess has increased considerably. Information that companies store digitally is vulnerable to data breaches by both malicious hackers and careless employees. The costs associated with these breaches can be staggering. Insurers responded to this new risk by offering cyber insurance products that specifically cover the risk of loss from data breaches and other cyber attacks. Cyber insurance products were also developed to provide coverage for the gap inherent in Commercial General Liability (CGL) policies for damage which is not tangible, along with the peripheral costs caused by cyber security breaches.

Many insurers entered the new cyber insurance market without conducting a systemic evaluation of the unique risk posed by each insured. Had they conducted an adequate evaluation, insurers would have asked effective questions and performed their due diligence. Using this information, underwriters would have been able to accurately assess the nature and extent of the risks being insured. Also, insurers would have been able to explain to their insureds how much insurance they should carry in order to avoid risking an unanticipated exhaustion of policy limits.

Because cyber insurance buyers and sellers both lack correct and adequate information regarding what they are getting in this new market, an information gap exists which creates the very conditions needed for a market based on illusions. Insurers, mesmerized by the allure of the new market, rushed to issue new cyber coverage products. That illusion was fortified by the fact that the market for cyber insurance products seemed extremely lucrative because by all appearances there was significant growth in what seemed to be a robust market. These insurers may be headed down a slippery slope fraught with catastrophic losses not anticipated by the underwriting process. On the demand side, potential cyber insurance customers have their own illusions. Some potential customers do not see cyber security as

Aaron J. Aisen is an attorney at Goldberg Segalla in New York and is a member of the firm's Global Insurance Services, Regulatory Compliance, and Cyber Risk and Social Media practice groups. Prior to joining Goldberg Segalla, he was a compliance investigations officer at a major international bank. There, he had hands-on experience with a variety of federal laws and regulations, with particular emphasis on the Bank Secrecy Act and the Patriot Act. His legislative and regulatory experience includes experience in three legislative offices, a district attorney's office, and a city law department. He previously interned for Justice Salvatore Martoche of the New York State Supreme Court, Appellate Division, Fourth Department and an administrative law judge with the New York State Division of Human Rights. He graduated with honors from the University at Buffalo Law School and he received his bachelor's degree from the George Washington University, where he concentrated his studies on conflict and security issues in international affairs. He also earned a master's degree in public administration from Brigham Young University, where he concentrated on financial and management analysis and graduated with distinction.

an issue that they need to address with a two-fold strategy: an adequate cyber security plan and adequate insurance in the event that a security breach occurs. These businesses may soon be faced with uninsured (or underinsured) losses from data breaches. Other businesses place too much faith in the cyber insurance they purchased. They think that if they have cyber insurance they can do little or nothing more to mitigate the risk of a data breach. Unfortunately, they may learn that relying exclusively on the policy proceeds as the primary tool in their proverbial cyber tool bag will turn out to be unwise because there is still so much uncertainty and confusion regarding the full extent of cyber risks and the type and extent of the risks covered by different policies.

Reality may be replacing illusions as new notification laws and regulations are forcing organizations to rethink their old policies of self-insuring breaches.[4] One example of these notification requirements is the new Securities and Exchange Commission (SEC) reporting requirements for publicly traded companies on their data security.[5] Insurers and insureds

---

[4] Matt Dunning, SEC Guidelines Drive Renewed Interest in Cyber Risk Insurance Coverage, Business Insurance (June 8, 2012 3:20 pm), http://www.businessinsurance.com/article/20120608/NEWS07/120609886 (last visited July 19, 2013).

[5] *Id.*

are discovering that the costs associated with a data breach are high, especially costs related to notifying affected consumers, legal expenses, and settlements.[6] In reality, these actual costs may be greater than reported because even though incidents of data breach are not new, experts think that cyber attacks have been under-reported due to the embarrassment and costs associated with notifying customers.[7]

Comprehensive underwriting standards for evaluating cyber risks are not available yet. Until the standards exist, determining the appropriate cost of coverage is seriously impeded. Because the nature and extent of the risk to be covered can vary significantly, insurers may not be able to fully comprehend the nature or extent of the risks they are underwriting and industry standards for adequate insurance coverage also may be underdeveloped. Unfortunately, companies that choose to forego cyber insurance coverage may be naïvely relying on inadequate data security measures or a false belief that a general CGL policy provides sufficient coverage. Those companies risk discovering that their security measures are inadequate and that their general liability policy does not cover their losses at all or that the coverage is inadequate.

Cyber coverage may well be the emperor's new clothes for both insurance companies and potential insureds if appropriate questions are not asked at the underwriting phase or, in the first instance, at the time a potential insured considers whether to purchase coverage. A lack of understanding as to the insured's security prevention or the insured's coverage needs could give rise to an unwelcome surprise for insurer and insured alike.

This Article proceeds in six parts. Part II describes the growing threat of cyber attacks and importance of cyber security. Part III explains the purpose of cyber insurance and the risks it covers. Part IV contains a thorough discussion of the market for cyber insurance including its growth, supply and demand features, and problem areas. Part V explains how the more developed European market for cyber insurance has addressed some of the problems associated with cyber insurance. It also includes a summary of findings regarding incentives and barriers for a cyber insurance market in Europe and how they can be useful when considering how to correct the market imperfections in the United States cyber insurance industry. In Part VI, we discuss case law regarding how courts have dealt with the issue of whether cyber claims are covered by traditional forms of insurance. A review of the case law also explains the coverage gap that cyber insurance can fill. In Part VII, we offer our recommendations regarding pricing and buying cyber insurance policies and integrating them into a comprehensive plan for managing cyber attack risks.

---

[6] Mark Greisiger, Cyber Liability & Data Breach Insurance Claims: A Study of Actual Payouts for Covered Data Breaches, NetDiligence (June 2011), http://www.netdiligence.com/files/CyberLiability-0711sh.pdf.

[7] World Economic Forum, Global Risks 2012 26 (2012), http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2012.pdf; Daniel Nelson, *Technology: Understanding the Ins-and-Outs of Cyber Insurance*, InsideCounsel (Sept. 28, 2012), http://www.insidecounsel.com/2012/09/28/technology-understanding-the-ins-and-outs-of-cyber.

II.
Cyber Attacks and Cyber Security

Cyber security is a hot topic with no shortage of written material discussing the subject, and for good reason. Technological advances have caused cyber security to become relevant to every aspect of our lives.[8] As personal and business information is consumed in the digital age, our dependence on cyber space has grown. Unfortunately, our vulnerability to loss increases dramatically when we entrust personal and proprietary information to third parties over whom we have no control. Significant aspects of our lives are held in electronic form by others and the security measures taken by such entities will determine our vulnerability to loss.

Cyber attacks are on the rise. Barry Buchman and Mickey Martinez of Gilbert LLP reported that "between 2005 and 2011, there were over 2300 data breaches, exposing over 535 million records at an average cost to the affected firms of $234 per compromised record. The surge in data breaches alone caused some commentators to label 2011 the 'Year of the Breach.'"[9]

It is not an overstatement to suggest that the digital world is under siege and that cyber attacks permeate all levels of international markets. The World Economic Forum identified cyber security as a major global risk for 2011 and 2012.[10] Richard Clarke, the former U.S. Special Adviser to the President of the United States on cyber security has said, "Every major company in the United States has already been penetrated by China."[11] FBI Director Robert Muller has said that "[i]n the not too distant future, we anticipate that the cyber threat will pose the number one threat to our country."[12] Indeed, the chances of a cyber breach are so

---

[8] National Security Council, *Cyber Security*, White House (May 29, 2009), http://www.whitehouse.gov/cybersecurity (last visited July 19, 2013).

[9] Barry Buchman and Mickey Martinez, *Importance of Procuring Cybersecurity Insurance Coverage*, Law360 (June 29, 2012 1:04 PM), http://www.law360.com/articles/354385/importance-of-procuring-cybersecurity-insurance-coverage (last visited July 22, 2013).

[10] World Economic Forum, Global Risks 2011 7 (2011), http://reports.weforum.org/wp-content/blogs.dir/1/mp/uploads/pages/files/global-risks-2011.pdf; Global Risks 2012, *supra* note 7, at 12.

[11] Rob Waugh, *'Every Major Company in the U.S. has been Hacked by China': Cyber-Espionage Warning from U.S. Security Chief Who Warned of 9/11*, The Daily Mail (Mar. 28, 2012), http://www.dailymail.co.uk/sciencetech/article-2121624/Every-major-company-U-S-hacked-China-Cyber-espionage-warning-U-S-security-chief-warned-9-11.html (last visited July 19, 2013).

[12] Jeb Boone, *FBI Warns Threat of Cyber Attacks on Par With Terrorism*, GlobalPost.com (Mar. 2, 2012), http://www.globalpost.com/dispatches/globalpost-blogs/the-grid/anonymous-fbi-al-qaeda-cyber-war-attacks (last visited July 22, 2013).

high that it is not a question of if, but when.[13] In September 2012, the White House computer system was attacked when an individual in the White House Military Office opened an email and clicked on the link to open the attachment.[14] As our awareness of this risk grows, cyber insurance has an undeniable appeal. Insureds are becoming acutely aware that cyber insurance coverage must be considered when discussing risk assessment and mitigation.

III.
Cyber Insurance

Much of the literature and professional commentary on the subject of cyber insurance is devoted to encouraging organizations to purchase cyber insurance against the eventuality of a data breach. Even government regulation is promoting the purchase of this product. For example, the SEC encourages publicly traded companies to give a "[d]escription of relevant insurance coverage," and, in some situations, requires disclosures regarding past cyber attacks and future threats.[15] Even the White House promoted cyber insurance stating the belief that "[i]nsurers will require a level of security as a precondition of coverage, and companies adopting better security practices often receive lower insurance rates."[16] In fact, one of the recommendations of this report is to "[r]equire government contractors to carry cyber-insurance [because d]oing this would improve cyber-security among government contractors...."[17]

---

[13] The Inkerman Group, *Not If, But When? Businesses and Cyber Security*, Inkerman (Apr. 2012), http://www.inkerman.com/assets/files/Articles%20and%20Reports/The%20Inkerman%20Group%20-%20Business%20and%20Cyber%20Security.pdf.

[14] Gerry Smith, *White House Hacked in Cyber Attack that Used Spear-Phishing to Crack Unclassified Network*, HuffingtonPost (Oct. 1, 2012 12:35 PM), http://www.huffingtonpost.com/2012/10/01/white-house-hacked-cyber-_n_1928646.html (last visited July 19, 2013).

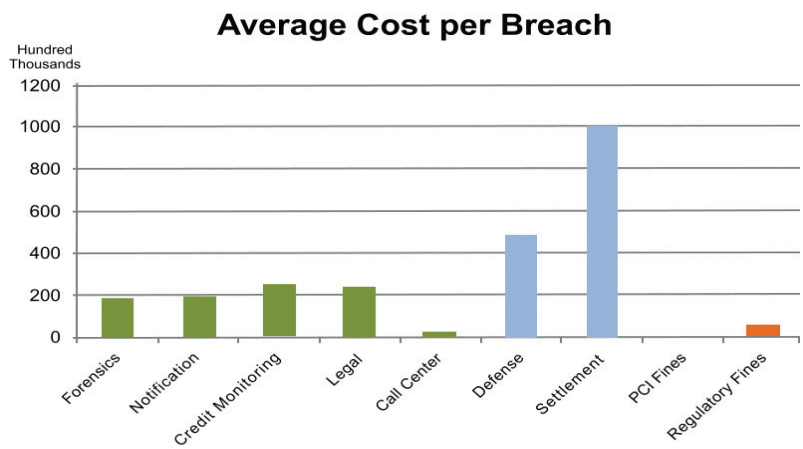
[15] Div. of Corporate Fin., Sec. & Exch. Comm'n, CF Disclosure Guidance: Topic No. 2 Cybersecurity (Oct. 13, 2011), *available at* http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[16] Larry Clinton, *Cyber-Insurance Metrics and Impact on Cyber-Security*, White House, 1 (undated), http://www.whitehouse.gov/files/documents/cyber/ISA%20-%20Cyber-Insurance%20Metrics%20and%20Impact%20on%20Cyber-Security.pdf (last visited July 23, 2013) [hereinafter *Cyber-Insurance Metrics*].

[17] *Id at* 8. This particular idea that the cyber insurance industry would ultimately drive organizations to make their systems more secure is also discussed in the academic literature. *See, e.g.* Jay P. Kesan, Rupterto P. Majuca & William J. Yurcik, *The Economic Case for Cyberinsurance* 9-11 (Univ. of Ill. Coll. of Law Working Paper No. 2, 2004), *available at* http://www.queensu.ca/dms/DMS_Course_Materials_and_Outline/Readings-MPA831/Cyberinsurance-831.pdf (discussing how cyber insurance might promote safer IT environments where the premium of the insurance is tied to safety measures an organization takes). Whether this is actually the case is still an open question. Given the fact that some insurance companies are not necessarily requiring these safeguards and audits to confirm the safeguards, the incentive to put the safeguards in is not there. This situation leads to increased risk for the insurance company and any reinsurers.

Cyber insurance generally covers two broad categories of risk associated with a data breach. First, such insurance "covers a business in case of unauthorized access or use of its computer network whether internally or externally."[18] Second, cyber insurance "protects a business that violates privacy laws or regulations that protect data from 'unauthorized eyes.'"[19] An organization can buy coverage for everything, or for a discrete group of risks associated with a cyber attack including, but not limited to business interruption, forensics, notification, credit monitoring, litigation, and settlement costs.

One recent study which examined cyber insurance claims for incidents between 2005 and 2010 provides a glimpse of long-term cost. This study, released by NetDiligence in June 2011, is entitled *Cyber Liability & Data Breach Insurance Claims: A Study of Actual Payouts for Covered Data Breaches*.[20] In this report, NetDiligence reviewed information on claims for 117 breaches, including 77 claims which contained a detailed itemization of the costs and indemnity paid. While this is a relatively small sample over a relatively short period, the data collected offers insight as to what we might expect to see in the future. Below is a graph which lays out the average payout by claim.[21]



Litigation and settlement costs were, by far, the largest costs associated with the payment of cyber liability and data breach claims.

---

[18] Casualty Actuarial Society, *Insurers Trying to Keep Up With New Cyber Liability Exposures*, Casact (June 29, 2012), http://casact.org/media/index.cfm?fa=viewArticle&articleID=2007(last visited July 22, 2013) [hereinafter CAS].

[19] *Id.*

[20] Greisiger, *supra* note 6.

[21] *Id.* at 5.

IV.
The Cyber Insurance Market

Reactions to the cyber insurance market are mixed and the statistical analysis of market response varies; however, the conclusions of most surveys are generally consistent. In a survey sponsored by Zurich, 35.1% of survey participants responded that they purchased cyber insurance, while 60.1% stated they had not.[22] Thirty-six percent of those that had not purchased cyber insurance were larger organizations defined by $1 billion or more in annual revenue.[23] Of those that did not purchase cyber insurance, 24.3% responded that they would purchase it in the next year, while 52% said they would not, and 23.6% responded they did not know if they would purchase cyber insurance.[24] As reported in the Zurich survey, companies may not purchase cyber liability insurance for one or more of the following reasons:

- They are investing in prevention rather than insurance.
- There are limited markets for cyber liability insurance.
- They experience broker disconnects when trying to purchase cyber liability insurance.
- They think cyber liability policies lack clear coverage.
- They lack information to make informed decisions.
- They think cyber liability policies are too expensive.
- They find the application process too difficult.
- They think deductibles are too high.
- They think costs and benefits are difficult to quantify.
- They think policy coverage is too limited.[25]

---

[22] Josh Bradford, *A New Era in Information Security and Cyber Liability Risk Management: A Survey on Enterprise-wide Cyber Risk Management Practices*, Advisen 8 (Oct. 2011), http://corner.advisen.com/pdf_files/cyberliability_riskmanagement.pdf .

[23] *Id.*

[24] *Id.*

[25] *Id.*

Other surveys present a less optimistic picture. One recent survey showed that only 28% of major United States companies have any form of cyber insurance.[26] More interestingly, 66% of those that do not have cyber insurance believe "they don't have significant data exposure, since they believe their internal controls are adequate."[27] Jane Taylor, a consulting actuary at Huggins Actuarial Services responded to the data by opining that it may be "hubris."[28] Taylor is not alone in this opinion.

Bruce Webster of Bruce F. Webster & Associates noted that many organizations experience a "Thermocline of Truth" as it pertains to IT.[29] Just as there is a defining line between the hot and cold water in a freshwater lake, those responsible for drafting corporate budgets often have little understanding of their company's IT system.[30] Corporate budgets are driven by a desire to increase profits which, by definition, requires that unnecessary costs must be cut where possible.[31] If management determines that its company's security measures are adequate to resist a potential data breach, the company's decision makers that set the budget will surely allocate company resources to other projects, initiatives or costs.[32] Webster also noted that, ironically, because of intellectual property and privacy concerns, many companies are hesitant to open their IT doors for review.[33]

Webster and Taylor's sentiments are supported by the Zurich survey. Nearly 72% of those responding to the survey said "information security risks are a specific risk management focus within their organization."[34] However, when asked, "In your experience, are cyber risks viewed as a significant threat to your organization?" only 45.3% said "yes" as to the Board of Directors, and only 57.9% said "yes" as to "C-suite executives."[35]

Such survey responses may well explain how the cyber response is organized. When asked "Which department is PRIMARILY responsible for spearheading the information security risk management effort?" nearly 75% of the respondents said it is the IT Depart-

---

[26] CAS, *supra*, note 18.

[27] *Id.*

[28] *Id.*

[29] Telephone Interview with Bruce Webster, Principal and Founder, Bruce F. Webster & Associates LLC (Sept. 13, 2012). (Bruce Webster is an internationally recognized expert in information technology. He has testified before Congress and given presentations all over the world, given private briefings to the U.S. intelligence community and representatives of other countries. He has also appeared several times in the media and is called upon as an expert witness in litigation. Bruce F. Webster, Brucefwebster.com, http://brucefwebster.com/about-bruce-f-webster/ (last visited July 27, 2013).

[30] *Id.*

[31] *Id.*

[32] *Id.*

[33] *Id.*

[34] Bradford, *supra* note 22, at 4.

[35] *Id.*

ment.[36] While the majority of survey participants acknowledged that mitigating cyber risk should be an enterprise-wide operation, only 57% of respondents said they had an information security risk team that was comprised of individuals from multiple departments.[37] This could give rise to other legal problems for such organizations. Survey results also included the following findings:

> More than two thirds of respondents said their organizations have a disaster response plan in place in the event of a major breach. For 41 percent of respondents, the role of the IT department includes fulfilling state data breach notification laws following a breach. This may represent a significant deficiency in emergency response planning. The IT department often is ill-equipped to interpret the notification requirements of dozens of states and to marshal the resources necessary to fulfill the requirements of each state following a major breach.[38]

This caused those conducting the Zurich survey to conclude:

> While most companies have implemented information security and cyber risk management programs, for the majority of these organizations, cyber insurance is not incorporated as part of the overall strategy for many. The growing interest in the coverage, however, is apparent with the increased number of companies that have purchased protection in recent years, or are planning on buying coverage in the near future.[39]

The Zurich report noted that since half of those that did not currently maintain cyber insurance were thinking about procuring it, the cyber insurance market may be a growth opportunity for brokers and insurers.[40] While the number of large companies with cyber insurance might be relatively small, the market is relatively large. Michael L. McCarthy of Axis Capital has estimated that cyber insurance generates approximately $500 million in premiums and that the market is growing at a steady rate of 10% to 25% annually with midsized and smaller companies making up a larger segment of customers.[41] Another source

---

[36] *Id.* at 7.

[37] *Id.* at 6.

[38] *Id.* at 9.

[39] *Id.*

[40] *Id.* at 8.

[41] CAS, *supra* note 18.

estimates that premiums were approximately $800 million in 2011.[42] As more organizations follow the trend and purchase cyber insurance several problems may arise.

More than thirty companies offer cyber insurance, but cyber insurance is a relatively new product and few claims have been paid under such policies.[43] This has resulted in inconsistent standards for determining how insurers evaluate risk and set appropriate premiums. Absent underwriting guidelines, it is problematic for insurers to set a fair premium without significant due diligence by insurers evaluating the risk presented by each insurance application. Significantly, a lack of due diligence could result in a premium which is unfair to the insurer and the insured, depending on the true nature of the risk. The potential exposure to insurers for this product is unknown because data regarding indemnity payments is undeveloped and, for that reason, the methodology for determining premiums is not consistent.[44]

Some insurers conduct due diligence as part of the underwriting process. John Merchant of Freedom Specialty Insurance Company noted that underwriters pay attention to certain things including the type and amount of data a customer has, internal controls, third party evaluations, and public filings,[45] especially with the new SEC regulations regarding publicly traded companies.[46] However, such due diligence is not consistent. Cyber insurance risk remains significant in light of the fact that premiums are not calculated on the basis of loss history and standards for rating such risk have not yet been established.

While a cyber insurance policy may appear to be a proper risk mitigation strategy, the placement and/or procurement of coverage requires appropriate, substantive questions in order to properly evaluate the risk for which coverage is sought. The failure to ask the right questions could lead to losses not expected by either the insurer or the insured. Attitudes reflected by responses to the Zurich survey suggest a number of problems.

First, the perception of the risk illustrated by the responses may well prevent potential data breach victims from buying the insurance. Second, if these organizations decide to purchase cyber insurance without proper due diligence as to their needs and potential exposures, there is no way to truly evaluate the nature of the risk for which coverage is sought and, therefore, it is difficult understand the appropriate type and amount of coverage to procure. Finally, without an audit that would reveal the purported insured's needs and potential risks, there could be a reduced incentive to implement security measures to mitigate the possibility of a data breach as part of an overall strategy to avoid exposure for such intrusions.

---

[42] Juliette Fairley, *Insurance Industry Responds to Cyber Attack Increase*, Insurance Networking News (Apr. 20, 2012), http://www.insurancenetworking.com/news/cyber-insurance-standards-zurich-cna-liberty-30256-1.html?zkPrintable=true (last visited on July 26, 2013).

[43] Eduard Kovacs, *ENISA Wants a Cyber Insurance Market for European Companies*, SoftPedia (June 29, 2012, 7:48 GMT), http://news.softpedia.com/news/ENISA-Wants-a-Cyber-Insurance-Market-for-European-Companies-278214.shtml (last visited on Nov. 5, 2012).

[44] Bradford, *supra* note 22, at 8.

[45] John Merchant, *Insurance of Cyber Liability* (June 4, 2012) (unpublished CAS Reinsurance Seminar Slides) (on file with the editor); CAS, *supra* note 18.

[46] Dunning, *supra* note 4.

V.
The European Approach

Analysis of the U.S. cyber insurance market warrants consideration of trends in the European market. European analysis of the cyber insurance market has taken into account issues that U.S. insurers and policy makers have either failed to consider, or have considered and chosen to ignore.

A. *The European View of Privacy*

As a background on the European regulatory environment, privacy is defined and articulated as a concept with greater priority in Europe than in America. Article 8 of the European Convention on Human Rights ("ECHR") is entitled the "Right to Respect for Private and Family Life."[47] Similarly, the Charter of Fundamental Rights of the European Union ("The Charter" or the "CFREU"),[48] is labeled in Article 7 as "Respect for private and family life."[49] Consistent with the notion that privacy must be a priority, Article 8 of the Charter states:

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.[50]

---

[47] Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, 213 U.N.T.S. 221, art. 8, *available at* http://www.echr.coe.int/Documents/Convention_ENG.pdf (last visited July 22, 2013).

[48] While the Charter is formally an EU document and formally published in the Official Journal C84 of 30 March 2010, the drafters based it off of "fundamental rights and freedoms recognized by the European Convention on Human Rights, the constitutional traditions of the EU Member States, the Council of Europe's Social Charter, the Community Charter of Fundamental Social Rights of Workers and other international conventions to which the European Union or its Member States are parties." *The Charter of Fundamental Rights of the European Union* European Parliament (Feb. 21, 2001), http://www.europarl.europa.eu/charter/default_en.htm (last visited Sept. 11, 2012).

[49] *The Charter of Fundamental Rights of the European Union (2010/C 83/02)*, Official Journal of European Communities 10 (Feb. 21, 2001), http://www.europarl.europa.eu/charter/pdf/text_en.pdf.

[50] *Id.*

In line with this emphasis on privacy, the EU published directive 95/46/EC on data privacy in 1995 with the introduction, "on the protection of individuals with regard to the processing of personal data and on the free movement of such data."[51] Because this was a directive, each member state was responsible for creating its own individual law to satisfy the requirements of the directive. For example, the United Kingdom passed the Data Protection Act 1998.[52]

B. *The Incentives and Barriers Report*

In June 2012, The European Network and Information Security Agency (ENISA) issued a report called *Incentives and Barriers of the Cyber Insurance Market in Europe* (Incentives and Barriers Report).[53] In this report, ENISA noted the interesting paradox of cyber insurance that, initially, there should not be a market for cyber insurance. The Incentives and Barriers Report states the following:

> Commonly, theoretical analysis usually portrays this in the context of the following three properties of cyber-risk:
>
> - *Interdependent security* – the risks faced by a firm depends not only on its own choices but also on those of others. As more firms decide not to invest in security, the probability of a successful terrorist attack [or data breach] grows, and there is no economic incentive for any specific firm to invest in security. As the number of firms/organisations gets large, a firm will not be willing to incur any costs to invest in security because it knows it will be contaminated by other unprotected firms;
> - *Correlated risk* – a supply side problem where the many potential losses from a single event can be so extensive as to force insurers not only to price contracts to accommodate these losses but also to protect against the possibility of themselves suffering ruin by multiple claims occurring at once. This is seen by some as being driven from monocultures of equipment (a single vulnerability affecting many) and therefore an opportunity for market intervention;

---

[51] Council Directive 95/46, 1995 O.J. (L 281) 31 (EC), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

[52] Data Protection Act, 1998, c. 29 (U.K.), *available at* http://www.legislation.gov.uk/ukpga/1998/29.

[53] *Incentives and barriers of the cyber insurance market in Europe*, ENISA (June 2012), http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/incentives-and-barriers-of-the-cyber-insurance-market-in-europe/at_download/fullReport [hereinafter *Incentives and Barriers Report*].

- *Information asymmetries* – specifically insurers lacking information on the risks that the insured may be bearing which can also lead to adverse selection (where the insurer cannot efficiently segment the market, leading to insurers inefficiently pricing premiums on the basis of the 'lowest common denominator'). This is compounded by the aspect of network externalities as a common characteristic of cyberspace related phenomena. The related aspect of moral hazard (where the insured may act in a more insecure manner by investing in less security after the acquisition of insurance because they now know that the insurer will bear some of the negative consequences) informs this consideration. In either case these situations reflect opportunistic behaviour on the part of either the supply or demand side of the market.[54]

For example, the United Kingdom is home to Lloyd's of London and is one of the world's financial centers. Market exposure (in terms of claims exposure) in the UK is approximately $250 million.[55] However, consistent with other statistics which illustrate a disconnect between premiums and risk, the gross written premiums for such coverage net approximately £3 to £4 million,[56] or approximately $4.87 million to $6.49 million. The estimate for the current size of the global market for premiums is approximately $500 to $700 million.[57] Michael McGavick of XL Insurance has estimated that the world market could be worth $1 billion.[58]

ENISA notes three concerns with regard to the incongruity of these figures. First, if an insurance company does not understand the risk, how can it accurately charge premiums which sufficiently reflect the risk? Second, in a market in which worldwide technology continues to grow rapidly, will a policy written today accurately reflect the technology as it continues to evolve throughout the policy period? Finally, with limited actuarial data, how can an insurer buy adequate reinsurance in the event of a catastrophic loss?[59]

Despite perceived, perhaps theoretical barriers, the cyber insurance market appears to have "taken off."[60] One cause for this explosive growth is regulation. The Incentives and Barriers Report cited an article on the Lloyd's website entitled *Rising Claims Reflect Cyber*

---

[54] *Id.* at 11-12 (footnotes omitted).

[55] *Id.* at 14.

[56] *Id.*

[57] *Id.*

[58] Mike McGavick, *Innovate or Risk Irrelevance*, Intelligent Insurer-Monte Carlo Today (Dec. 12, 2012), http://content.yudu.com/A1yg18/MCTWednesday/resources/index.htm?referrerUrl= (last visited July 26, 2013).

[59] *Incentives and Barriers Report*, *supra* note 53, at 19.

[60] *Id.* at 14 (internal quotation marks omitted).

Concerns of Multi Nationals,[61] which identifies a number of factors driving the claims including the increased use of technology and the growing sophistication of hackers.[62] However, the most significant driver of the market is likely regulation. Paul Bantick, a cyber underwriter at Beazley, opined that "[t]he cyber insurance market has really taken off in recent years in the U.S. where demand has grown with strengthened legislation."[63] Bantick also added, "Demand for cyber insurance is growing among UK and European companies, as the changing regulatory environment and recent high profile data breaches are increasing awareness."[64] This sentiment was echoed by Jeremy Smith, a broker at Willis who stated, "At Willis we have seen a 56% increase in cyber claim notifications in the past year. This rise is reflecting the evolving environment and a growing dependency on IT systems."[65] NetDiligence's survey results support these facts and figures.[66]

Laws are changing in the EU. Currently, the data protection framework can be found in Directive 95/46/EC; however, because it is a directive, each EU member state has flexibility as to how to implement the directive.[67] The EU is moving toward increased uniformity with regard to the implementation of such directives, perhaps best illustrated by a proposal for General Data Protection Regulation, which could create uniform notification requirements across the EU if it goes into effect.[68] Such new requirements are addressed in Articles 30, 31, and 32 of the new General Data Protection Regulation.[69] The regulation also addresses a loophole in the 1995 directive which limited personal data breach notifications to the electronic communications sector.[70]

ENISA made four recommendations in the Incentives and Barriers Report. First, "[c]ollect empirical evidence on the use of cyber-insurance products in Europe, including the types of products purchased, types of risk insured, premiums, payouts etc. in order to thoroughly determine the current and future market trends in this domain."[71] This empiri-

---

[61] *Id.* at 14; *Rising Claims Reflect Cyber Concerns of Multi Nationals*, Lloyd's (Sept. 16, 2011), http://www.lloyds.com/news-and-insight/news-and-features/market-news/industry-news-2011/rising-claims-reflect-cyber-concerns-of-multi-nationals (last visited July 23, 2013) [hereinafter *Rising Claims*].

[62] *Rising Claims, supra* note 61.

[63] *Id.*

[64] *Id.*

[65] *Id.*

[66] Greisiger, *supra* note 6.

[67] Morey Elizabeth Barnes, *Falling Short of the Mark: The United States Response to the European Union's Data Privacy Directive*, 27 Nw. J. Int'l L. & Bus. 171, 178 (2006).

[68] Barbara Daskala, Dr. Marnix Dekker & Christoffer Karsberg, *Cyber Incident Reporting in the EU: An overview of security articles in EU legislation*, ENISA 3 (Aug. 2012), *available at* http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/cyber-incident-reporting-in-the-eu.*Id.*

[69] *Id.*

[70] *Id.* at n. 4.

[71] *Incentives and Barriers Report, supra* note 53, at 3.

cal data is needed to adequately assess risk and ensure that the premium is commensurate with that risk, regardless of the reasons for the increase in purchases of cyber insurance. Second, ENISA suggests strengthening the regulatory framework to encourage companies to prevent data breaches rather than rely primarily on cyber insurance.[72] Third, ENISA recommends consideration of frameworks to help firms appraise the value of information.[73] These frameworks may help risk managers determine how to accurately assess how cyber insurance will play a role in their risk management strategy. It may also assist underwriters in deciding what premiums to assess. Finally, they suggest considering the government as the insurer of last resort.[74]

VI.
Coverage for Cyber Risks Under Traditional Policies

Prospective cyber insurance policyholders need to understand the limited scope of coverage which may be available for cyber losses under CGL policies. Many policyholders operate under the mistaken belief that the CGL policies will provide coverage in the event of a data breach. However, since not all CGL policies are written to provide the same or similar coverage, CGL policyholders must be cautious when determining the scope of coverage, if any, under their general liability policy.

In this Part, we discuss the most significant case law regarding coverage for data breaches under traditional forms of insurance. These cases are also instructive regarding issues which may exist in the future with regard to the cyber risk insurance products that are starting to be introduced to the market.

A. *The Sony PlayStation Case: Zurich v. Sony*

The seminal case on the issue of coverage under a general liability policy for a data breach is *Zurich v. Sony*.[75] In April 2011, several of Sony's systems, including its "PlayStation" system were hacked and credit card numbers were stolen.[76] It is estimated that over 100 million individuals had personal information stolen and this data breach resulted in several class action suits.[77] Sony sought to have its insurer, Zurich, defend and indemnify it against these suits.[78] However, Zurich filed a declaratory judgment action against Sony seeking a judicial determination that no coverage was owed.[79]

---

[72] *Id.*

[73] *Id.*

[74] *Id.*

[75] Compl. for Declaratory Judgment at 5-6, Zurich v. Sony, No. 651982/2011 (N.Y. Sup. Ct. July 20, 2011), 2011 WL 2905600.

[76] *Id*.

[77] *Id.* at 6-8.

[78] *Id.* at 8.

[79] *Id.* at 16-17.

Zurich asserted that the underlying claims pertaining to losses for a data breach did not allege property damage within the insuring clause of the Zurich policy.[80] While this case has not yet been decided, other cases are instructive as to how the court may rule.

B. *"You've Got Mail": AOL v. St. Paul Mercury Insurance Co.*

Consider *America Online, Inc. v. St. Paul Mercury Insurance Co.,* a case in which America Online (AOL) was sued by customers claiming that AOL 5.0 had damaged their computers.[81] Specifically, the customers alleged that AOL 5.0 caused physical damage to, and loss of use of, customers' tangible property in the form of computers, computer data, software, and systems.[82] AOL tendered the suit to its insurer, St. Paul Mercury Insurance (St. Paul), seeking coverage under its CGL policy.[83]

Since the St. Paul policy expressly covered loss to "tangible property," the issue before the court was whether computer data, software and systems are tangible property. AOL argued these items are tangible property because they are "capable of being realized."[84] The court held that "computer data, software, and systems" are not tangible property.[85] The court noted that the Multidistrict Litigation complaint alleged loss of use of the consumers' computers, not that the computer itself was "physically damaged."[86] The court concluded the injury alleged fell squarely within the label of "property which isn't physically damaged" under the impaired property exclusion.[87]

The impaired property exclusion provided that harm to property that is not physically damaged is excluded from coverage where it is caused by a faulty or dangerous product. The court noted:

> Finally, the allegations of harm to consumers' computers run squarely into the common law economic loss rule. At bottom, the underlying complaint alleges that AOL 5.0 is a defective component incorporated into a larger product, the consumers' computers. Any damages stemming from the loss of computer use are purely economic, do not constitute harm to property other than the integrated product, and are thus not recoverable under any tort theory.[88]

---

[80] *Id.* at 8-16.

[81] 207 F. Supp. 2d 459 (E.D. Va. 2002).

[82] *Id.* at 461.

[83] *Id.*

[84] *Id.* at 466.

[85] *Id.*

[86] *Id.* at 470.

[87] *Id*.

[88] *Id*. at 462.

The court further noted that "[f]inding that computer data and software is intangible is also consistent with the long line of precedent holding that ideas, information, and designs are not tangible property."[89]

The court held that physical damage to the computer is not the same as the loss of the use of the computer and that the plain language of the policy required "physical damage," defined as "'relating or pertaining to the body, as distinguished from the mind, soul or the emotions.'"[90] The court noted that the computer data and systems are the "brains" of the computer.[91]

In affirming, the Fourth Circuit held:

> [T]he conclusion that physical magnetic material on the hard drive is tangible property is quite separate from the question of whether the data, information, and instructions, which are codified in a binary language for storage on the hard drive, are tangible property. Certainly the hard drive itself is a medium in which the data, information, and instructions are stored, but the data itself must be considered apart from the medium. Thus, if a hard drive were physically scarred or scratched so that it could no longer properly record data, information, or instructions, then the damage would be physical, affecting the medium for storage of the data.[92]

The court continued:

> But if the arrangement of the data and information stored on the hard drive were to become disordered or the instructions were to come into conflict with each another, the physical capabilities and properties of the hard drive would not be affected. Such disordering or conflicting instructions would amount to damage to the data and information and to the instructions (i.e., the software) but not to the hard drive. The magnetic material on the hard drive could be reoriented and reordered with reinstallation of the instructions. So it is that we make the distinction between hardware and software.[93]

C. *The Fourth Circuit's Approach: American Guaranty v. Ingram*

The Fourth Circuit's ruling in the AOL case has not been accepted in all jurisdictions. In *American Guaranty & Liability Insurance Co. v. Ingram Micro, Inc.,*[94] Ingram Micro's

---

89 *Id*. at 468.

90 *Id*. at 469 (quoting Black's Law Dictionary 794 (1991)).

91 *Id.*

92 America Online, Inc. v. Saint Paul Mutual Ins. Co., 347 F.3d 89, 95 (4th Cir. 2003).

93 *Id*.

94 2000 WL 726789 (D. Ariz. 2000).

data center in Tucson experienced a power outage "caused by a ground fault in the fire alarm panel."[95] While the building still had electric power and was not disrupted, "all of the electronic equipment at the Data Center, including the computers and telephones, stopped working."[96] The United States District Court for the District of Arizona found that "'physical damage' is not restricted to the physical destruction or harm of computer circuitry but includes loss of access, loss of use, and loss of functionality."[97]

To reach this conclusion, the court reviewed the federal code and the penal laws of several states and observed that while these were not insurance statutes, "[l]awmakers around the country have determined that when a computer's data is unavailable, there is damage; when a computer's services are interrupted, there is damage; and when a computer's software or network is altered, there is damage."[98] The court concluded that "[r]estricting the policy's language to that proposed by [the plaintiff] would be archaic."[99] It should be noted that while this rationale and decision was criticized in *America Online, Inc. v. St. Paul Mercury Insurance Co.*,[100] *American Guarantee* was not appealed.

D. *The Eighth Circuit's Approach: Eyeblaster v. Federal Insurance Co.*

Some courts have taken the middle ground regarding CGL coverage for cyber losses. For example, in *Eyeblaster Inc. v. Federal Insurance Co.*,[101] David Sefton said that when he used one of Eyeblaster's products, spyware uploaded and "caused his computer to immediately freeze up."[102] Sefton sued Eyeblaster and Eyeblaster in turn sued Federal Insurance in order to force Federal to defend against the Sefton suit.[103]

In deciding the case, the Eight Circuit agreed generally with the Fourth Circuit in how they define physical property. The Eighth Circuit said:

> The General Liability policy Eyeblaster purchased from Federal obligates the insurer to provide coverage for property damage caused by a covered occurrence. Property damage means "physical injury to tangible property, including resulting loss of use of that property…; or loss of use of tangible property that is not physically injured." The definition of "tangible property" excludes "any software, data or other information that is in electronic form."[104]

---

[95] *Id.* at *1.

[96] *Id*.

[97] *Id*. at *2.

[98] *Id.* at *3.

[99] *Id*.

[100] Amer. Online, Inc. v. St. Paul Mercury Ins. Co., 207 F. Supp. 2d 459, 469-70 (E.D. Va. 2002).

[101] 613 F.3d 797 (8th Cir. 2009).

[102] *Id.* at 800.

[103] *Id.*

[104] *Id.* at 801.

The court then largely agreed with the Fourth Circuit's analysis in *America Online* that without physical damage to the computer, the plaintiffs had to claim "physical injury to the hardware in order for Eyeblaster to have coverage for 'physical injury to tangible property.'"[105]

The court noted that the policy also included coverage under the second clause which stated "loss of use of the tangible property that is not physically injured."[106] Sefton claimed in his suit against Eyeblaster that "his computer was 'taken over and could not operate,' 'froze up,' and would 'stop running or operate so slowly that it will in essence become inoperable.'"[107] Federal argued that an exclusion in the General Liability Policy for "Damage to Impaired Property or Property Not Physically Injured" precluded them from having to pay the claim.[108] The exclusion read: "This exclusion does not apply to the loss of use of other tangible property resulting from sudden and accidental physical injury to your product or your work after it has been put to its intended use."[109] Federal pointed to the definition of the term Impaired Property in the policy:

> [T]angible property other than your product or your work, that cannot be used or is less useful because:
>
> - it incorporates your product or your work that is known or thought to be defective, deficient, inadequate or dangerous; or
> - you have failed to fulfill the terms or conditions of a contract or agreement;
>
> if such property can be restored to use by:
>
> - the repair, replacement, adjustment or removal of your product or your work; or
> - your fulfilling the terms or conditions of the contract or agreement.[110]

The court rejected this argument noting that "no evidence exists that the computer can be restored to use by removing Eyeblaster's product or work from it."[111] The court further explained:

---

[105] *Id.* at 802.

[106] *Id.* at 801-02 (internal quotation marks omitted).

[107] *Id.* at 802.

[108] *Id*.

[109] *Id.*

[110] *Id.* at 802-03.

[111] *Id.* at 803.

> Sefton alleges that the website that he believes caused the damage to his computer "was owned and operated by Eyeblaster or person's [sic] or entities that are controlled directly or indirectly by Eyeblaster." Such a broad characterization does not suffice to satisfy the requirement that Eyeblaster incorporated its product or work into Sefton's computer.[112]

In this case, the court recognized the differences between tangible and intangible property, and because of the language of the policy found that the policy did not cover damage to intangible software. In contrast, coverage existed for the damage to the computer caused by the spyware.

E. *Computer Fraud Riders to Blanket Crime Policies: The DSW Case*

In *Retail Ventures Inc. v. National Union Fire Insurance Co. of Pittsburgh, PA,*[113] National Union Fire Ins. Co. (National Union) denied coverage under a computer fraud rider to a blanket crime policy for losses DSW Shoe Warehouse (DSW) and its affiliates sustained as a result of a computer hacking scheme that compromised customer information. The court considered, among other things, whether the plaintiffs suffered a loss resulting directly from the theft of insured property by computer fraud.[114]

Directly after the breach, the plaintiffs "incurred expenses for customer communications, public relations, customer claims and lawsuits, and attorney fees in connection with investigations by seven state Attorney Generals and the Federal Trade Commission."[115] As a result of the FTC investigation, the plaintiffs entered into a consent decree which required them to "establish and maintain a comprehensive information security program designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers."[116] In addition, DSW lost over $4 million from compromised credit card information, such as "costs associated with charge backs, card reissuance, account monitoring, and fines imposed by VISA/MasterCard."[117]

The policy included "Computer & Funds Transfer Fraud Coverage"[118] which provided coverage for any loss sustained by the insured directly from theft of any [i]nsured property by Computer Fraud."[119] However, the policy also contained three exclusions which stated that the policy did not apply:

---

[112] *Id.*

[113] 691 F.3d 821 (6th Cir. 2012).

[114] *Id.* at 824.

[115] *Id.*

[116] *Id*.

[117] *Id.*

[118] *Id.* at 826.

[119] *Id.*

> (k) to the defense of any legal proceeding brought against the Insured, or to fees, costs or expenses incurred or paid by the Insured in prosecuting or defending any legal proceeding whether or not such proceeding results or would result in a loss to the Insured covered by this Policy, except as may be specifically stated to the contrary in this Policy;
>
> . . .
>
> (m) to damages of any type for which the Insured is legally liable, except direct compensatory damages arising from a loss covered under this Policy;
>
> (n) to costs, fees and other expenses incurred by the Insured in establishing the existence of or amount of loss covered under this Policy.[120]

The court of appeals noted that, with the exception of the clause dealing with compensatory damages, the exclusions limited first-party claims and were largely silent on third-party claims.[121]

National Union also denied coverage under a policy exclusion which stated that coverage does not apply to any loss of proprietary information, trade secrets, confidential processing methods, or other confidential information of any kind.[122] The court rejected this argument, holding that proprietary information is information which is held solely by the insured.[123] Here, the stolen information was held by the insured, the insured's customers, their banks, other financial institutions, as well as other merchants.[124] Therefore, such information could not be considered proprietary.[125]

National Union also claimed the exclusion "other confidential information of any kind"[126] covers information belonging to anyone who is expected to be protected from unauthorized disclosure, and which would include not only the other terms in this exclusion, but also the coverage for computer fraud.[127] Again, the court disagreed with National Union and noted that other terms in the exclusion referred to things which were internal to DSW and gave DSW "an opportunity to obtain advantage over competitors who do not know or use the information."[128] So, the term "other confidential information of any kind" referred to other

---

[120] *Id.* at 827.

[121] *Id.*

[122] *Id.* at 832.

[123] *Id.* at 833.

[124] *Id.*

[125] *Id*.

[126] *Id.* at 832.

[127] *Id.* at 834.

[128] *Id*.

information that dealt with how the business was operated, which would not include the stolen credit card information.[129]

It is noteworthy that although *National Union* was decided in 2012, it was based on an event that occurred seven years earlier. The cyber insurance industry and the cyber insurance products on the market have changed considerably since 2005. Also, *National Union* considered such issues with regard to a computer fraud rider to a crime insurance policy. Albert E. Lietzau V, of Cyber Risk Solutions, noted, "Often, general liability policies will have a flat-out exclusion that says 'We will not cover any sort of cyber-liability information loss[.]'… So if a customer or client wants to make sure they're fully protected, they shouldn't rely on just a general liability or crime policy."[130] Mr. Lietzau's admonition is appropriate with regard to *National Union* because the court's analysis pertained to a policy covering activities similar to those covered by cyber insurance. *National Union* demonstrates the challenge of policy interpretation with regard to such policies and losses.

VII.
Pricing and Buying Cyber Insurance: Some Recommendations

It would be unwise to expect that a typical CGL policy provides coverage in the event of a data breach and, for that reason, the cyber insurance market is growing rapidly; however, the procurement of a cyber risk policy is also fraught with danger. Insureds and insurers must understand the specific nature of the risk for which coverage is sought; otherwise, one of the parties to the insurance policy could face exposure which was not anticipated at the time of underwriting the risk. The insured and the insurer must understand the risks sought to be covered so that coverage is appropriate for the unique circumstance of the insured's business.

What kind of questions should an organization ask when deciding to purchase cyber insurance? John Proctor of Gartner Inc. notes that most literature on cyber insurance encourages organizations to buy cyber insurance.[131] However, Proctor also encourages organizations to avoid the hype because many authors writing about cyber insurance are in the "supply chain" for cyber insurance.[132]

---

[129] *Id.*

[130] Ericka Chickowski, *Fluke DSW Win Shouldn't Erase Breach Insurance Needs*, Dark Reading (Sept. 5, 2012), http://www.darkreading.com/database-security/167901020/security/news/240006829/fluke-dsw-win-shouldn-t-erase-breach-insurance-needs.html (last visited July 26, 2013).

[131] Eric Chabrow, *10 Concerns When Buying Cyber Insurance,* Bank Info Security (June 14, 2012), http://www.bankinfosecurity.com/10-concerns-when-buying-cyber-insurance-a-4859/op-1 (last visited July 23, 2013).

[132] *Id.*

Purported insureds need a solid risk management plan for their IT systems. First, insureds should perform a comprehensive review of their IT systems.[133] Proctor suggested that, as part of this review, organizations must determine the type of coverage needed and which coverage will provide coverage for the risks anticipated by the insured.[134] Don Fergus, an IT risk consultant and the 2012 chairman of the IT Security Council for ASIS, a security professionals' organization, gave this advice:

> The IT people and the risk people desperately need to get together to talk about risk in terms of information technology and the likelihood and outcomes of a breach occurring.… Information professionals, especially information security leaders, need to step up. They need to understand that they're in charge of more than just security. They need to understand and articulate the vulnerabilities that they face in terms of risk."[135]

Cyber insurance can be relatively expensive. As of January 2012, the range of cost for cyber insurance was $7,000 to $40,000 per millions of dollars of loss."[136] "With losses possibly totaling in the tens – or even hundreds of millions of dollars, getting a policy able to cover such costs can present a staggering additional cost in insurance premiums."[137] Proctor suggests that when an organization considers the purchase of a cyber policy, the organization must find a broker that "has experience with actually working with clients who filed claims, not somebody reading the back of the policy to see what's in it."[138] In short, there may be no substitute for experience.

Proctor noted that cyber policies contain a litany of exclusions. So, before buying a policy, an organization should understand the type of breaches to which it may be vulnerable and procure coverage for such breaches.[139] Organizations that use cloud-based services should also determine whether such services are covered and how this might affect any coverage for non-cloud items.[140] Similarly, many in the insurance industry do not understand cyber security issues, especially with respect to the processing the claims.

---

[133] Mary K. Pratt, *Cyber insurance offers IT peace of mind – or maybe not*, Computer World (Jan. 13, 2012 6:00 AM), http://www.computerworld.com/s/article/9223366/Cyber_insurance_offers_IT_peace_of_mind_or_maybe_not?taxonomyId=17&pageNumber=1 (last visited July 23, 2013).

[134] Chabrow, *supra* note 131.

[135] Pratt, *supra* note 133.

[136] *Id.*

[137] *Id.*

[138] Chabrow, *supra* note 131.

[139] *Id.*

[140] *Id.*

An organization must be educated about what is and is not covered. Proctor cites the example of an organization with an advanced firewall but has it turned off.[141] Having the protection is simply not good enough. Further, does the organization understand what types of breaches might be covered? If an employee accidentally downloads a virus, is that covered? Is there only coverage for a cyber attack from an outside source?[142]

After noting the many exclusions which may be included in a cyber policy, Proctor observed that companies must be meticulous when completing cyber insurance application surveys. In short, do not make a misrepresentation on the insurance application. If an organization claims to have a firewall on its application and it does not, a claim may not be paid. If an organization represents on the insurance application that it has an 8-digit alphanumeric password policy, but does not require employees to follow the password policy, a claim might be denied.[143]

Those who consider purchasing cyber insurance coverage should bear in mind that it is a new product. Relatively few claims have been made and although insurers say that they pay claims, there is no statistical data that documents their history of paying cyber insurance claims.[144] In this regard, Proctor cautions, "If you have significant cyber insurance and experience a loss … you still may have a fight on your hands."[145]

VIII.
Conclusion

A few questions go a long way when procuring cyber coverage. Insurers and insureds must carefully consider the nature of the risk, the vulnerability of an insured to a data breach, and the potential costs which could arise if a breach occurs. In addition, procuring a cyber policy must be just one component of an overall risk strategy plan, rather than a safety net that the insured relies upon to make it whole in the event of a data breach. Just as an investment counselor might recommend a diverse investment portfolio, an insured must implement a diverse program to protect itself from a data breach in the digital age.

A cyber audit should be part of any risk management program. Taking appropriate steps to implement preventative measures from a data breach must be part of a strong risk management infrastructure. The infrastructure should not consist of only the IT department. Rather, an appropriate risk management culture must be perpetuated by the CEO and Board of Directors. In short, organizations must better analyze how cyber insurance fits with the company's overall risk management strategy.

---

[141] *Id*.

[142] *Id*.

[143] *Id*.

[144] *Id*.

[145] *Id*.

Conversely, insurers must better understand the specific needs and vulnerabilities of each potential insured in the underwriting process. A one-size-fits-all insurance application could miss the mark in evaluating the risk presented by a particular business. An appropriate evaluation of the risk of a particular insurance application may allow the insured (and the insurer) to avoid the embarrassment of walking down the street in a cloak of security which covers nothing, but was procured because it sounded like a good idea at the time.

The Federation of Insurance Counsel was organized in 1936 for the purpose of bringing together insurance attorneys and company representatives in order to assist in establishing a standard efficiency and competency in rendering legal service to insurance companies, and to disseminate information on insurance legal topics to its membership. In 1985, the name was changed to Federation of Insurance and Corporate Counsel, thereby reflecting the changing character of the law practice of its members and the increased role of corporate counsel in the defense of claims. In 2001, the name was again changed to Federation of Defense & Corporate Counsel to further reflect changes in the character of the law practice of its members.

The FEDERATION OF DEFENSE & CORPORATE COUNSEL QUARTERLY, published quarterly through the office of publication by the Federation of Defense & Corporate Counsel, Inc., 11812 North 56th Street, Tampa, FL 33617.

Manuscripts and correspondence relating to the submission of articles for possible publication should be sent to the Editor-in-Chief, Susan M. Popik, 38 Woodhill Drive, Redwood City, CA 94061 or emailed to smpopik@gmail.com. All other correspondence should be directed to the Executive Director.

The FDCC is pleased to provide electronic access to Quarterly articles from 1997 to present at its Internet website, www.thefederation.org.