June 2012

BRC

THE BETTERLEY REPORT

CYBER/PRIVACY INSURANCE MARKET SURVEY – 2012:

Surprisingly Competitive, as Carriers Seek Market Share

Richard S. Betterley, CMC
President
Betterley Risk Consultants, Inc.

Highlights of This Issue

- *Specialized Products Continue to be Designed for Market Segments*
- *Newer Carriers Forcing Incumbents to Offer Higher Sublimits*
- *Rates Remain Competitive*
- *Carriers Push Down the Cost of Breach Response Services*
- *Safe Harbors for Certified Protected Health Care Information*

Next Issue

August
Private Company Management Liability Insurance Market Survey 2012

Editor's Note: *In this issue of The Betterley Report, we present our annual review and evaluation of insurance products designed to protect against the unique risks of data security for organizations. Risks could include the breach of security by a hacker intent on stealing valuable data, or simple release of data through the carelessness of an employee or vendor.*

The intense interest in cyber security and the insurance industry's response to it has been paralleled by the proliferation of vendors offering ways to minimize the risk of data breach and loss. One company, InfoGard Laboratories, has identified an opportunity for data holders in the healthcare industry to benefit from HHS Safe Harbor protections if they adhere to certain data security standards. We are pleased to include an article describing this important protection from Mac Brinton, InfoGard's President, as a part of this year's Cyber/Data Privacy Insurance Market Survey.

List of Tables

Social media has become a focus of liability for some insureds and their advisors; although there are few claims arising out of social media, the dramatic rise in Facebook, LinkedIn, Twitter, and others is fueling interest in coverage. For many insureds and their brokers, 'cyber' means the Internet, so cyber coverage must mean insurance for bad things that happen on the Internet.

Cyber carriers are responding to this interest by offering media liability coverage options in their policies. In order to try to sort through these coverages, last year we added three new Media Liability tables for our readers. In retrospect, we think that was too much detail, and have condensed the tables to a single one.

Note that this Report does not focus on coverage for technology providers that support e-commerce, such as Internet Service Providers, technology consultants, and software developers. That market is reviewed in our February issue, Technology E&O Market Survey.

One thing we would like to point out is the difficulty in separating Technology products from Cyber Risk products; for many carriers, the same base product is used, then adapted to fit the Technology Service Provider insured or the Cyber Risk insured. Where the carrier has a separate product, we reviewed here their Cyber Risk product; if it is a common base product, we included information about both.

We have tried to eliminate the sometimes confusing table columns which were more appropriate to a technology product. With the help of many of the carriers we cover, we identified coverage elements that had little relevance to a non-tech services provider. We think this makes this Report more usable and a bit more compact (although it is still our most lengthy Report).

Information in this Report includes information provided by participating insurance companies. Professional counsel should be sought before any action or decision is made in the use of this material. Copyright 2012 Betterley Risk Consultants, Inc. No part of this publication or its contents may be copied, downloaded, stored in a retrieval system, further transmitted or otherwise used in any form other than with the expressed written permission of Betterley Risk Consultants, Inc.

In looking at our information, if you see that a certain carrier's policy does not include, for example, Errors & Omissions coverage, keep in mind that this coverage is most important to a service provider and that the same carrier might have a separate product for those insureds. You will probably find that product reviewed in our February issue.

The types of coverage offered by Cyber Risk insurers vary dramatically. Some carriers offer coverage for a wide range of business activities, while others are more limited. For the insured (or its advisors) looking for proper coverage, choosing the right product is a challenge.

Most of the carriers offer multiple Cyber Risk products, so crafting the coverage for each insured requires the best in risk identification and knowledge of the individual covers. More than most insurance policies, Cyber Risk requires experienced risk professionals to craft the proper coverage. The insurance industry still needs to do a better job of helping brokers understand the exposures, coverage, and services of Cyber Risk, so that they can better serve their clients. Many brokers may have only a general knowledge of Cyber exposures and coverage.

We have tried to present a variety of coverages to illustrate what is available in the market. Thirty-one sources of insurance are included in this survey. These carriers (and in a few instances, Managing General Underwriters) represent the core of the Cyber Risk insurance market. Last year's survey covered twenty-nine, and the 2010 Report only included nineteen sources of product.

Carriers added to our coverage in 2012 are Argo Pro, Berkley, and RSUI. We have removed Euclid, as that market is only available to insureds that buy Technology E&O. Euclid is still included in our February Tech E&O Market Survey.

Although liability, data extortion, and crisis management coverage are important, it isn't going too far to say that privacy risk is driving the market for Cyber Risk coverage. Carriers are tweaking the products to improve coverage, while in some instances adding protection against adverse claims experience, especially in the remediation costs area. This is interesting to us, as our clients generally seem to feel that a liability loss is not likely, but that the remediation coverage is useful. As carriers tweak their remediation coverages, they face a challenge of continuing to offer obviously helpful protection without incurring excessive losses.

Some of this tweaking includes arranging deeply-discounted breach response services; these services can be as effective as those that an insured might arrange on its own, but at a much lower cost. We applaud this added value provided by some insurers, and hope to see it made more widely available. Insureds sometimes prefer to make their own selection of providers, but the

Companies in This Survey

Ace
Admiral
Allied World
Arch
Argo Pro
Axis
Beazley
Berkley
Brit
CFC
Chartis
Chubb
CNA
Crum & Forster
Digital Risk
The Hartford
Hiscox
Ironshore
Liberty International
Markel
NAS
Navigators
OneBeacon
Philadelphia
RLI
RSUI
Safeonline
ThinkRisk
Travelers
XL
Zurich

Information in this Report includes information provided by participating insurance companies. Professional counsel should be sought before any action or decision is made in the use of this material. Copyright 2012 Betterley Risk Consultants, Inc. No part of this publication or its contents may be copied, downloaded, stored in a retrieval system, further transmitted or otherwise used in any form other than with the expressed written permission of Betterley Risk Consultants, Inc.

cost benefit of using the prenegotiated services shouldn't be ignored.

Finally, a reminder that, while each insurance carrier was contacted in order to obtain this information, we have tested their responses against our own experience and knowledge. Where they conflict, we have reviewed the inconsistencies with the carriers. However, the evaluation and conclusions are our own.

Rather than reproduce the carriers' exact policy wording (which of course can be voluminous), we in many cases have paraphrased their wording, in the interest of space and simplicity. Of course, the insurance policies govern the coverage provided, and the carriers are not responsible for our summary of their policies or survey responses.

In the use of this information, the reader should understand that the information applies to the standard products of the carriers, and that special arrangements of coverage, cost, and other variables may be available on a negotiated basis.

For updated information on this and other Betterley Report coverage of specialty insurance products, please see our blog, The Betterley Report on Specialty Insurance Products, which can be found at: **www.betterley.com/blog**.

Introduction

As with all of our Market Surveys, Cyber Risk coverage represents a new or recently developed form of coverage designed to address the needs of new risks confronting organizations. Cyber Risk coverage epitomizes new insurance products, presenting insurance product managers with challenges as they learn what their insured's need, and what the carriers can prudently cover.

Most carriers were convinced that their best opportunities are to sell Cyber Risk coverage to mainstream companies that have significant Cyber Risk exposures. Many of those prospective insureds are already the carrier's customers, looking for coverage not present in traditional policies. The experience of a distressingly large number of major companies in the past few years is perhaps only the tip of the iceberg representing the threat of data theft facing businesses worldwide. Insurance protection to backstop IT security safeguards must be carefully considered for businesses and institutions such as hospitals, educational institutions, and public entities.

Carriers have developed very different products to address what they think Cyber Risk companies need; we have provided a Product Description table that lets the carrier describe in its own words the coverage it is offering. This table is vital to the reader's understanding of the various - and varied - products offered.

Specialized Cyber Risk insurance comes in a variety of forms, but we find it most helpful to divide coverage into property, theft, or liability for surveying purposes. Some carriers offer liability only products, while others offer a combination of property, theft, and liability cover.

Carriers are offering Cyber Risk enhancements to existing policies, such as Business Owners, Management Liability, and other policies. We don't cover that product segment in this Report, although we do cover it in our Private Company Management Liability Report (August).

Information in this Report includes information provided by participating insurance companies. Professional counsel should be sought before any action or decision is made in the use of this material.
Copyright 2012 Betterley Risk Consultants, Inc. No part of this publication or its contents may be copied, downloaded, stored in a retrieval system, further transmitted or otherwise used in any form other than with the expressed written permission of Betterley Risk Consultants, Inc.

State of The Market

The market continues to broaden, especially in health care and the small- to mid-sized insureds segments. Health care systems and their vendors in particular are buying Cyber Risk (and in the case of vendors, often buying Technology E&O) at a rapid clip. Carriers are offering specialized products to these insureds.

In addition to health care, carriers report much of their growth coming from small- to mid-sized companies newly aware of the possibilities of liability, and especially a breach and resulting response costs, arising out of the possession of private data. This is leading to a large increase in policy count, but far less in new premium written.

Annual premium volume information about the U.S. Cyber Risk market is hard to come by, but in reviewing the market, we have concluded that the annual gross written premium is in the $1 billion range (up from $800 million in last year's Report). Growth has been dampened by some rate competition as new carriers try to gain market share, and much of the growth has come from smaller insureds. A lot more business is being written, but at slightly lower rates and for much smaller insureds.

Still, we think that this market has nowhere to go but up – as long as carriers can still write at a profit. The proliferation of data breaches and the increasing sensitivity of the public to protection of their private data surely means increasing levels of claims. Perhaps offsetting this increase in claims will be the opportunity to respond to breaches more cost effectively, as carriers negotiate lower response costs and law firms get more competitive in their pricing.

Privacy coverage is clearly driving the market; Cyber Risk seminars and conferences are packed with prospective customers, carriers, brokers, and attorneys interested in privacy risk, coverage, and services. Interest is translating into purchases, which we (and many others) have been predicting. Management may still be thinking 'it can't happen here' but as more events occur that would be covered, more Cyber Risk insurance is being bought.

Data breaches have become disturbingly frequent, especially over the past few months. We are unsure if this is a result of increased reporting (breaches happened before but were not disclosed) or increased activity by, and effectiveness of, hackers, but it is going to have an impact on the insurance market.

What might those impacts be? Possibly higher interest in coverage as more potential insureds see the frequency of breaches, but also higher premium rates and/or retentions, as the increasing frequency of claims are paid for (and as insurance company leadership sees breaches occurring even at "good" risks).

We can imagine the conversations in insurance company management meetings about cyber insurance after reading about breaches at companies such as Lockheed Martin, Sony, and Citibank. And even worse - RSA SecureID token breaches.

We think that a strong influence on the purchase of Cyber Risk insurance is the increasing awareness of the value of post-breach response coverage. We have spoken with many CFOs,

Information in this Report includes information provided by participating insurance companies. Professional counsel should be sought before any action or decision is made in the use of this material. Copyright 2012 Betterley Risk Consultants, Inc. No part of this publication or its contents may be copied, downloaded, stored in a retrieval system, further transmitted or otherwise used in any form other than with the expressed written permission of Betterley Risk Consultants, Inc.

Treasurers, and Risk Managers who are not so sure that the case for liability protection has been made, but that can easily see how post-breach costs would be a burden.

We also asked carriers about the health and interest of the reinsurance market that supports Cyber Risk products, and they generally reported that reinsurers still like the product. Increasing interest in Cyber Risk product support was reported by the responding carriers. There is a great deal of concern over accumulation risk (that is, the same cause of loss affecting multiple insureds, leading to massive claims), which has caused reinsurers to limit their exposure. With much data moving to the cloud, this accumulation risk is becoming more severe, a trend that concerns us greatly.

Most carriers report strong growth in premium. Although we must maintain confidentiality about the details, carriers that have been significant players in the Cyber Risk market for at least several years indicate premium growth ranged from 25% to over 100%. Only one of these carriers reports growth of over 100%, but several others report between 50% and 100%. Most were in the 10-25% range, and only two were under 10%. This is impressive, considering the difficult economic conditions many insureds were operating in.

Newer carriers are reporting strong rates of growth, but this is off of relatively small base premiums, of course. These newer carriers are helping expand the market with innovative product features as they seek to create a presence in what has become a crowded segment. In our consulting, we have seen several instances where incumbent carriers greatly expanded their limits only as a result of the threat of being replaced by newer entrants to the Cyber Risk insurance market.

Premium volumes were well reported to us in this survey. We know that at least two carriers are writing a relatively large amount of business (well over $50 million), with other carriers writing in the $10-25 million range. Others are fairly far behind; there are numerous markets writing under $5 million, but few in the $5-10 million range.

Finally, as noted, there are a number of carriers that are offering Cyber Risk coverages as an option to another policy, such as a package policy, Management Liability policy, or some other mainstream product. We did not include these products in this Report but have added more specific questions to our Private Company Management Liability Market Survey 2011 (August).

State of the Market – Rates and Retentions

We asked the carriers whether they planned rate increases (or decreases) during the upcoming year, and what they expected of their competitors. Most offered their thoughts, which were similar to what we heard in 2011, despite the onset of a slowly hardening commercial insurance market.

Rates for Cyber Risk insurance, unlike the traditional commercial insurance lines, are still showing signs of softness. Some of the markets writing relatively low volumes of premium report plans to reduce rates on the order of 5%, while the larger carriers indicate that rates will stay flat or perhaps down a bit (5%). Several reported that they expect

Information in this Report includes information provided by participating insurance companies. Professional counsel should be sought before any action or decision is made in the use of this material. Copyright 2012 Betterley Risk Consultants, Inc. No part of this publication or its contents may be copied, downloaded, stored in a retrieval system, further transmitted or otherwise used in any form other than with the expressed written permission of Betterley Risk Consultants, Inc.

their competitors will reduce rates slightly further, but we are not so sure that will be the case.

The rates are soft at least in part because Cyber Risk is a new market with a great deal of growth potential; we surmise that carriers are trying to avoid missing the growth opportunity present in this still new product. Also, since new products tend to start with conservative rates, there may be room to lower them as the market learns more from its (loss) experience.

We do have some concern that the claims for post-breach response costs are turning out to be more common and more expensive than carriers might have expected. What was perhaps seen as a bit of a sweetener to the product is turning out to be a major source of claims. These claims could drive rates up, but we suspect that they are more likely to result in tighter cost controls by the carriers. As insurers learn more about how to respond to a breach at a lower cost, there is hope that rate increases can be held down.

Capacity and Retentions

Significant liability capacity exists, and higher limits can probably be stacked up if desired. Several of the carriers in this survey are willing to sit as excess over primary coverages.

Reasonable (account appropriate) retentions or deductibles are available. Deductibles or retentions can be quite competitive; the table shows minimums, of course. Large retentions ($500,000+) should be expected for larger insureds. We are not seeing carriers changing their deductible or retention strategy, generally willing to continue the levels of retentions they have been offering. The exception might be the smaller-sized insureds, which are being offered even lower deductibles than before.

Data Privacy

We are often asked whether coverage in a Cyber Risk policy includes losses arising out of data breaches. Coverage for costs resulting from data breaches often existed in Cyber policies, although not specifically spelled out. Because prospective insureds (and their advisors) wanted to see coverage more clearly stated, and because underwriters wanted more control over this evolving (exploding?) risk, more specific coverage has evolved.

Based on our research into privacy exposures and coverage, we have identified six key areas that should be considered:

- Types of Coverage and Limits Available
- Coverage Provided
- Coverage Triggers
- Types of Data Covered
- Remediation Costs Covered
- Remediation Coverage Services

The Types of Coverage and Limits Available

There are three fundamental coverage types: liability for loss or breach of the data, remediation costs to respond to the breach, and coverage for fines and/or penalties imposed by law or regulation.

Liability coverage is pretty self-explanatory - protection for the insured should it be sued for

Information in this Report includes information provided by participating insurance companies. Professional counsel should be sought before any action or decision is made in the use of this material. Copyright 2012 Betterley Risk Consultants, Inc. No part of this publication or its contents may be copied, downloaded, stored in a retrieval system, further transmitted or otherwise used in any form other than with the expressed written permission of Betterley Risk Consultants, Inc.

negligence leading to a security breach. Often the coverage does not explicitly list data breach as covered, rather including coverage as a part of a more general coverage grant for, as an example, failing to prevent unauthorized access to its computer system.

Some carriers offer more explicit coverage, such as an act, error, or omission that results in a theft of data from a computer system. Both methods can work, but it is very comforting to see a term like Theft of Data included in the coverage grant.

Coverage Provided

Coverages fall into three categories varying widely between the carriers:

- Liability – defense and settlement costs for the liability of the insured arising out of its failure to properly care for private data
- Remediation – response costs following a data breach, including investigation, public relations, customer notification, and credit monitoring
- Fines and/or Penalties – the costs to investigate, defend, and settle fines and penalties that may be assessed by a regulator; most carriers do not provide this coverage, although there can be coverage for defense costs.

Coverage Triggers

Coverage can be triggered by:

- Failure to secure data
- Loss caused by an employee
- Acts by persons other than insureds
- Loss resulting from the theft or disappearance of private property (such as data that resides on a stolen laptop or missing data storage media)

Types of Data Covered

Some carriers specify the types of data covered, others do not. Specific types covered can include:

- An individual's personally identifiable information
- Nonpublic data, such as corporate information
- Nonelectronic data, such as paper records and printouts

Remediation Costs Covered

Remediation is an area that is no longer new for Cyber Risk insurance (in fact, we believe that it is the primary reason why many insureds buy Cyber Risk insurance). This coverage is for the costs of responding to a data breach. Organizations that suffer a data loss may be required to notify their customers with notice of the data loss, which can be expensive. Typically, they may also want to mitigate the negative impact on their reputation by providing credit monitoring services for those same customers; this cost can also be significant.

Remediation cost coverage is now offered by most carriers. It can include:

- Crisis management services
- Notification of potentially affected customers
- Credit monitoring
- Costs to resecure (that is, make secure again) data

The frequency and impact of data breaches is widely discussed, with industry authority

Information in this Report includes information provided by participating insurance companies. Professional counsel should be sought before any action or decision is made in the use of this material. Copyright 2012 Betterley Risk Consultants, Inc. No part of this publication or its contents may be copied, downloaded, stored in a retrieval system, further transmitted or otherwise used in any form other than with the expressed written permission of Betterley Risk Consultants, Inc.

Ponemon Group estimating breach response costs of $194 per record in 2011 (source: 2011 Cost of Data Breach Study: United States; released March 2012). While this indicates a welcome decline from 2010 ($214 per record), it is still an indicator of the substantial cost involved for an organization that holds a large number of records.

We think that the number of breaches may be understated in the media, and asked Doug Pollack of data breach management firm ID Experts for his thoughts. According to ID Experts:

The ubiquity of data breach incidents is typically misunderstood. This is partially due to the fact that until recently only health care providers were required to report incidents that result in an unauthorized disclosure of private personal information to regulatory authorities.

Since reporting of health care data breaches began in September 2009, there have been 435 events that affected 500 or more individuals, and an astounding 42,000+ data breaches affecting less than 500 individuals. This highlights a little known phenomenon, that the vast majority of data breaches affect a reasonably small number of people.

If one extrapolates this situation more broadly across industries, the likelihood is that this represents the tip of an iceberg, in that there are massive numbers of small data breaches that go undetected and unreported. And to make things worse, while many of these breaches are benign and cost the breached organization very little, often under $10 per individual exposed, the potential cost from small data breaches can be very significant.

To illustrate, Massachusetts General Hospital was fined $1 million by the Department of Health and Human Services for a data breach affecting only 192 patients, because of the sensitive nature of the exposed data (patients diagnosed with infectious diseases) combined with a total lack of effective privacy and security measures.

To further look at the frequency and extent of data breaches across industries, the recently released Verizon Business report on data breaches (Verizon, April 2012) highlights 855 data breach incidents during 2011 that represented 174 million compromised records. They note that the somewhat recent phenomenon of "hacktivism" represents a significant trend that is contributing to the growth in the number of data breaches and the associated number of exposed records.

In this report, 54% of data breach incidents were in the accommodation and food services industry, 20% in retail trade, 10% in finance and insurance, and 16% in other industries. Given that the majority of these breaches exposed a material number of consumer records (average 203,000 per incident), one must assume that there exists a very significant number of data breaches in these industries that go undetected and/or unreported.

My expectation is that as regulatory enforcement actions continue to become more commonplace, and significant in terms of fines and penalties, the smaller data breach incidents that are currently living in the shadows will be increasingly reported and demonstrate more of the true extent of the overall data breach situation.

Doug Pollack can be reached at 971-242-4724 or doug.pollack@idexpertscorp.com

We think that Doug Pollack makes a good point, that the frequency of data breaches is understated. What will be the impact on Cyber insurers as more breaches are reported and as more organizations are insured for breach response costs? Are there more breaches than insurers realize?

Information in this Report includes information provided by participating insurance companies. Professional counsel should be sought before any action or decision is made in the use of this material. Copyright 2012 Betterley Risk Consultants, Inc. No part of this publication or its contents may be copied, downloaded, stored in a retrieval system, further transmitted or otherwise used in any form other than with the expressed written permission of Betterley Risk Consultants, Inc.

And will the prevalence of Cyber insurance make breaches more visible?

Remediation Coverage Services

There can be great benefit to the insured if the remediation services are prenegotiated and prepackaged; much like kidnap and ransom coverage, knowing how to respond to a loss can be daunting.

Carriers often offer prepackaged and prenegotiated services provided by third-party vendors. In some cases the insured is required to use designated vendors. In addition, some policies require the written consent of the carrier to use the services. Finally, a few of these services have a time limit for use, especially credit monitoring.

Security Assessment Requirements

Carrier-required assessments of the prospective insured's security policies are rare now; the details are in the accompanying table. Typically, but not always, any required assessment is free to the applicant.

Such an assessment can be very useful to the applicant, even if they do not buy the coverage. But if they do, a favorable assessment should help lower the insured's premium.

Requirements often differ depending on whether the coverage is first-party or third-party, and can also vary depending upon the type of business the insured is in. Some assessments are as simple (and easy on the applicant) as a review of its website, while others require an onsite review by third-party firms. Of course, the scale and intensity of the assessment is dependent not only on the carrier's underwriting philosophy, but also the nature and role of the applicant's business being considered.

Coverage

Property and Theft

The insurance industry offers property and theft (first-party) coverage and liability (third-party) coverage; some carriers offer liability only, while others offer all. We expect that more carriers will soon be offering combined property and liability programs.

First-party coverage protection against denial of web services (hacker attacks) is still a hot topic due to continuing attacks on leading Internet sites. Most property products cover this risk, although subject to negotiation and individual underwriting.

Theft exposures are sometimes not well understood in Cyber Risk risk assessments. The potential for traditional theft of money or goods *via* the Internet is often recognized, but theft or destruction of data, extortion, and theft of computing resources sometimes are not.

Liability

The definition of Insured differs on many policies, but special requirements can usually be met. Many carriers do not automatically include subcontractors as insureds, although many can endorse coverage.

The definition of a claim also varies significantly, with some carriers going to great lengths to define a claim, others using wording such as "a demand seeking damages."

Information in this Report includes information provided by participating insurance companies. Professional counsel should be sought before any action or decision is made in the use of this material.
Copyright 2012 Betterley Risk Consultants, Inc. No part of this publication or its contents may be copied, downloaded, stored in a retrieval system, further transmitted or otherwise used in any form other than with the expressed written permission of Betterley Risk Consultants, Inc.

Coverage for liability arising out of alleged media offenses has become a popular addition to Cyber policies. As many insureds and their brokers take Cyber activities to mean "Internet" activities, accompanied by buzz about social networking, questions about coverage for libel, slander, and intellectual property are increasing. 'Where is the coverage?' asks many an insured.

Some coverage may already exist in the Personal Injury portion of an existing General Liability policy, but more specific – and broader - coverage may be obtainable in a Cyber policy.

This Report includes a table that summarizes the (optional) Media Liability coverage that they might offer a Cyber Risk insured. It includes information as to whether:

- Coverage applies to all types of media, or is restricted to social media only, and
- Intellectual Property Rights that may be covered

Claims Reporting, ERP Options, and Counsel

Each liability policy reviewed is a claims made form so Extended Reporting Period (ERP) options are important; look for bilateral extended reporting period wording.

Selection of counsel continues to be a delicate issue with insureds, but as we frequently see in other new lines of coverage, carriers typically reserve the right to select, or at least approve, counsel. However, some carriers offer an option for the insured to preselect counsel, while others allow selection from an existing panel,

As with all questions of counsel choice, we recommend that insureds discuss and agree with their carrier beforehand on the counsel they want to use.

Generally, carriers can impose the infamous "hammer clause" on lawsuits that an insured may not want to settle. The use of "soft" hammer clauses is beginning to become prevalent in this product line

Specific Coverages Included in Policy

We have identified ten specific coverages that may be, but are not always, included in a Cyber Risk policy. These are:

- Virus
- Unauthorized Access
- Security Breach
- Personal Injury
- Advertising Injury
- Loss of Use
- Resulting Business Interruption
- Copyright Infringement
- Trade or Servicemark Infringement
- Patent Infringement

Generally, insureds should be careful to review their exposures to these types of losses, and make sure they use carriers that are willing to offer the needed protections. Coverage for Patent Infringement, for example, is rarely (if ever) offered in basic Cyber Risk forms, but can be purchased from a limited number of carriers as a separate Intellectual Property policy (as covered in Intellectual Property and Media Liability Market Survey April 2012).

Information in this Report includes information provided by participating insurance companies. Professional counsel should be sought before any action or decision is made in the use of this material. Copyright 2012 Betterley Risk Consultants, Inc. No part of this publication or its contents may be copied, downloaded, stored in a retrieval system, further transmitted or otherwise used in any form other than with the expressed written permission of Betterley Risk Consultants, Inc.

Exclusions

Exclusions are many and varied, as would be expected; please read those tables carefully. The tables have been simplified by removing exclusions primarily related to Technology E&O.

Rather than try to recite them here, the information for each carrier is found in the Exclusions table.

Risk Management Services

Carriers continue to augment the exposure identification and loss prevention services they offer their insureds. This is a tough area to operate in, because the range of e-commerce activity is extensive, not lending itself to a "one size fits all" approach.

We are pleased that carriers have identified these services as valuable to their insureds (and to their own loss ratios, we hope) and continue to broaden and strengthen their capabilities. More e-commerce-specific exposure identification and loss services are becoming available to insureds and their brokers. Services range from underwriting assessments that are shared with insureds through self-help audits and technical information to training, seminars, and testing by third-party service providers.

Please also refer to our discussion of privacy-related remediation services earlier in this Report.

Summary

Since we last wrote about the Cyber Risk insurance product in June of 2011, we have seen a substantial increase in the number of policies being bought and in the number of carriers entering the market. Further market segmentation has occurred as carriers adapt their standard policies to industries such as health care and exposures such as the cloud.

The market is still competitive – while insureds may be seeing rate increases on other lines of coverage, Cyber is still looking to conquer new markets, and price is an important decision point for potential insureds. Whether that is because carriers are buying market share or because rates have proven to be higher than claims is not known to us, but we suspect market share. Still, carriers seem to be behaving responsibly as to pricing, and that is a good thing.

The trend to prenegotiated breach response costs is also a good thing, providing breached companies with a way to secure the same services at a lower cost than they would have found if they didn't have insurance (or bought from a carrier that did not have prenegotiated response prices).

And finally, Risk Management services are evolving in support of the idea that it is always better to avoid a loss when possible – even better than having insurance to pay the claim. But insurance is still useful, and we expect to see a lot more of it being bought by organizations concerned about the proliferation of data breaches.

With that thought in mind, we are pleased to include the following article on data breach safe harbor protections written for *The Betterley Report* by Mac Brinton, President of InfoGard Laboratories.

Information in this Report includes information provided by participating insurance companies. Professional counsel should be sought before any action or decision is made in the use of this material. Copyright 2012 Betterley Risk Consultants, Inc. No part of this publication or its contents may be copied, downloaded, stored in a retrieval system, further transmitted or otherwise used in any form other than with the expressed written permission of Betterley Risk Consultants, Inc.

HHS Safe Harbor Protection from Data Breach Reporting as a Risk Reduction Tool

Maclynn Brinton
President
InfoGard Laboratories, Inc.

Trading in private medical information is a lucrative fraud. According to Larry Clinton, president and CEO of Internet Security Alliance, a stolen medical identification number can be sold for $50, compared to $1 for a stolen Social Security number. In 2011 the frequency of data breaches at health organizations jumped 32 percent from 2010, costing the industry an estimated $6.5 billion, as documented by a study released in December 2011 by the Ponemon Institute LLC, an information/security research group based in Traverse City, Michigan.

The vulnerability of electronic medical records to criminals has galvanized governmental regulatory bodies determined to better protect data storage systems. Health care organizations managing unsecured Protected Health Information (PHI) are subject to Data Breach Reporting requirements and penalties administered by the U.S. Department of Health and Human Services (HHS) Office of Civil Rights (OCR). Guidelines and punishments are stipulated by the Interim Final Rule (IFR) published in the Federal Register, Aug. 24, 2009, and are enforced. The OCR implements spot-check audits to monitor Health Insurance Portability and Accountability Act (HIPAA) compliance efforts.

Fortunately, HHS provides a safe harbor that protects against the need for reporting and the imposition of penalties for breaches if the organization meets certain data security standards. This safe harbor is a significant opportunity for health care organizations to lower the risk of damage to their reputation and to avoid substantial costs.

What is the HHS Safe Harbor from Breach Reporting?

The IFR provides a Safe Harbor from reporting and penalties if system owners have secured Protected Health Information in compliance with the requirements defined in the 2009 ruling. Securing PHI – including protection of data in motion, at rest, being processed, and being destroyed – must be accomplished according to the National Institute of Standards and Technology (NIST) security assurance requirements in the IFR.

Is Safe Harbor Certification Difficult to Achieve?

Evaluating compliance with NIST recommendations requires expertise in both cryptography and security. Only testing and certification by a qualified authority adept at cryptography can assure that a technology satisfies Safe Harbor requirements. Fortunately for health care organizations, technology certification can be accom-

Information in this Report includes information provided by participating insurance companies. Professional counsel should be sought before any action or decision is made in the use of this material. Copyright 2012 Betterley Risk Consultants, Inc. No part of this publication or its contents may be copied, downloaded, stored in a retrieval system, further transmitted or otherwise used in any form other than with the expressed written permission of Betterley Risk Consultants, Inc.

plished relatively easily, by installing certified, commercially available, off-the-shelf security products, then having the data system tested by an approved security laboratory. Certification that a health care organization qualifies for a Safe Harbor requires only the laboratory's confirmation that the previously certified security technology has been properly implemented.

How is Safe Harbor Certification Best Achieved?

Meeting security requirements is an increasingly

Potential Cost of Breach Response	*Safe Harbor Certification Benefit*
▪ Breach penalty from the U.S. Department of Health and Human Services (HHS) Office of Civil Rights (OCR) ▪ Penalty for non-compliant security discovered at a surprise audit by the OCR ▪ Legal assistance required to negotiate OCR penalties ▪ Public relations assistance required to comply with OCR mandatory media announcements ▪ Legal assistance directing Breach Response behavior	Completely eliminated by Safe Harbor
Damage to reputation	Completely eliminated by vigilant effort via installing protections mandated by the recognized authority: the National Institute of Standards and Technology (NIST)
Effort to prepare Breach Response Plan and coordinate plan execution if breach occurs	Completely eliminated by Safe Harbor
Required C-Level Executive involvement	Completely eliminated by removal of all complex major issues
Legal assistance to address potential liability litigation	Significantly reduced; NIST protections provide the recognized defendable security standards that HIPAA does not provide.
Forensics	▪ Significantly less likely to be required with NIST protections ▪ Can be accomplished without OCR dictates ▪ Reduced effort, experts are familiar with the protections
Remediation	▪ Significantly less likely to be required with NIST protections ▪ When required, the effort is reduced because experts are familiar with NIST protections

Information in this Report includes information provided by participating insurance companies. Professional counsel should be sought before any action or decision is made in the use of this material. Copyright 2012 Betterley Risk Consultants, Inc. No part of this publication or its contents may be copied, downloaded, stored in a retrieval system, further transmitted or otherwise used in any form other than with the expressed written permission of Betterley Risk Consultants, Inc.

complex task, but the protections necessary to qualify for Safe Harbor can be applied selectively. Addressing the most vulnerable aspects of a network is relatively inexpensive and provides compelling benefits in increased security and lowered financial risk. In the Ponemon Institute study, 49 percent of queried health organizations reported that lost or stolen devices caused their data breaches. Safe Harbor from Breach Reporting for these devices can be achieved for a very low cost.

What are the Benefits of a Safe Harbor Certification?

Safe Harbor Certification assures health care organizations of three major benefits:

- All costs associated with a potential data breach response are completely eliminated or radically reduced.
- The likelihood of a data breach is significantly diminished.
- In the very unlikely case of a lawsuit, an extremely important benefit is specified by the Safe Harbor – installation of the NIST breach protections provide the defendable security standards that HIPAA is missing.

Conclusion

Securing technologies storing and transmitting Protected Health Information is cost-effective, allowing organizations to avoid federal regulatory penalties, legal fees, and damage to reputation. With certification, an organization can be assured that a Data Breach is extremely unlikely, and that the implemented security standards guarantee a strong defense from any legal liability in the rare chance that a breach should somehow occur. For the most vulnerable aspects of a network, Safe Harbor Certification is relatively inexpensive and provides compelling benefits in increased security and lowered financial risk. Insureds, insurers, and their advisors should consider Safe Harbor Certification as a proven method of risk reduction.

Maclynn Brinton is co-founder and President of InfoGard Laboratories, Inc., headquartered in San Luis Obispo, Calif., and serving clients worldwide. Mac can be reached at 805-783-0810 or mbrinton@infogard.com

Information in this Report includes information provided by participating insurance companies. Professional counsel should be sought before any action or decision is made in the use of this material. Copyright 2012 Betterley Risk Consultants, Inc. No part of this publication or its contents may be copied, downloaded, stored in a retrieval system, further transmitted or otherwise used in any form other than with the expressed written permission of Betterley Risk Consultants, Inc.

About The Author

Richard S. Betterley, CMC, is the President of Betterley Risk Consultants, an independent insurance and alternative risk management consulting firm. BRC, founded in 1932, provides independent advice and counsel on insurable risk, coverage, alternatives to traditional insurance, and related services to corporations, educational institutions, and other organizations throughout the U.S. It does not sell insurance or related services.

Rick is a frequent speaker, author, and expert witness on specialty insurance products and related services. He is a member of the Professional Liability Underwriting Society and the Institute of Management Consultants. He joined the firm in 1975.

Rick created *The Betterley Report* in 1994 to be the objective source of information about specialty insurance products. Now published 6 times annually, *The Betterley Report* is known for its in-depth coverage of Management Liability, Cyber Risk, Privacy, and Intellectual Property and Media insurance products.

More recently, Rick created *The Betterley Report* Blog on Specialty Insurance Products, which offers readers updates on and insight into insurance products such as those covered in *The Betterley Report*. It provides him with a platform to more frequently and informally comment on product updates and newly announced products, as well as trends in the specialty insurance industry. www.betterley.com/blog

Information in this Report includes information provided by participating insurance companies. Professional counsel should be sought before any action or decision is made in the use of this material. Copyright 2012 Betterley Risk Consultants, Inc. No part of this publication or its contents may be copied, downloaded, stored in a retrieval system, further transmitted or otherwise used in any form other than with the expressed written permission of Betterley Risk Consultants, Inc.

Data Included in the Complete Report

You are reading the *Executive Summary* of this Market Survey. The *complete report for subscribers* includes numerous tables, such as:

- Contact Details, including:
  - Name and Title of Product Manager or (equivalent)
  - Mailing Address
  - Phone #
  - Email
- Target Markets for Each Carrier
  - Size
  - Industry Sector
  - Prohibited Industries
  - Prohibited States
- Summary Information about Each Product
- Limits, Deductibles, and Commissions
- Key Policy Terms, Definitions and Exclusions
- Risk Management Services

The Betterley Report is distributed by International Risk Management Institute, Inc. (IRMI) and may be accessed by subscribers on IRMI Online. To order this report, or the five other reports, call IRMI Client Services at (800) 827–4242 or visit **www.IRMI.com/Products**.

Information in this Report includes information provided by participating insurance companies. Professional counsel should be sought before any action or decision is made in the use of this material. Copyright 2012 Betterley Risk Consultants, Inc. No part of this publication or its contents may be copied, downloaded, stored in a retrieval system, further transmitted or otherwise used in any form other than with the expressed written permission of Betterley Risk Consultants, Inc.

The Betterley Report

The Betterley Report, your independent guide to specialty insurance products, is a series of six comprehensive reports published annually. Each report exhaustively reviews a single hot specialty insurance product, providing essential information such as:

- Who are the leading carriers?
- Complete contact information
- Target and prohibited markets
- Capacity, deductibles, and commission ranges
- Sample premiums (where available)
- Critical coverage and claims differences
- Exclusionary language
- Risk management services

The Betterley Reports are produced annually, and range from 50 to 175 pages in length. Current analyses include:

- Cyber and Privacy Risk Policies
- Technology Risk Insurance
- Employment Practices Liability Insurance (EPLI)
- Private Company Management Liability
- Side A D & O Liability
- Intellectual Property and Media Liability

The Betterley Reports are a huge timesaver for busy risk management professionals who need to be up-to-date on insurance products for their clients. Need to identify and evaluate the coverage, capacity and contacts for your clients? Need the best analysis of leading edge insurance products? We've done the ground work for you!

The Betterley Report is distributed by International Risk Management Institute, Inc. (IRMI) and may be accessed by subscribers on IRMI Online. To purchase a subscription, call IRMI Client Services at (800) 827-4242 or learn more on IRMI.com.

Betterley Risk Consultants is an independent insurance and alternative risk management consulting firm. Founded in 1932, it provides independent advice and counsel to corporations, educational institutions, and other organizations throughout the U.S. It does not sell insurance nor provide insurance-related services.

Betterley Risk Consultants, Inc.
Thirteen Loring Way • Sterling, Massachusetts 01564-2465
Phone (978) 422-3366 • Fax (978) 422-3365
Toll Free (877) 422-3366
e-mail rbetterley@betterley.com

The editor has attempted to ensure that the information in each issue is accurate at the time it was obtained. Opinions on insurance, financial, legal, and regulatory matters are those of the editor and others; professional counsel should be consulted before any action or decision based on this matter is taken. Note: all product names referred to herein are the properties of their respective owners.

The Betterley Report is published six times yearly by Betterley Risk Consultants, Inc. This material is copyrighted, with all rights reserved. ISSN 1089-0513

Information in this Report includes information provided by participating insurance companies. Professional counsel should be sought before any action or decision is made in the use of this material.
Copyright 2012 Betterley Risk Consultants, Inc. No part of this publication or its contents may be copied, downloaded, stored in a retrieval system, further transmitted or otherwise used in any form other than with the expressed written permission of Betterley Risk Consultants, Inc.