June 2014

BRC

THE BETTERLEY REPORT

CYBER/PRIVACY INSURANCE MARKET SURVEY – 2014:

"Maybe Next Year" Turns Into "I Need It Now"

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

Highlights of This Issue

- *Growth In All Areas of the Market*
- *Customer/Client Demands for Vendor Cyber Insurance Lead to Growth but Also Confusion*
- *Two Bonus Articles:*
  - *Rick Betterley on The Future of Cyber Insurance*
  - *Mike Naclerio and Jeremy Henley on the Virtual Privacy Expert*

Next Issue

August
Private Company Management Liability Insurance Market Survey 2014

Like What You See in this Executive Summary?

IRMI Risk & Insurance
KnowledgeBase • Education • Community

You won't believe the value in the full reports. Now Available on **IRMI® Online** and **ReferenceConnect™**

The Betterley Report provides insightful insurer analysis on these six markets and coverage lines:

- Cyber/Privacy Insurance Market Survey
- Technology Errors & Omissions
- Employment Practices Liability Insurance
- Side A D&O Liability Insurance
- Private Company Management Liability Insurance
- Intellectual Property and Media Liability Insurance

Each annual report provides a comprehensive review (50 to 175 pages) with numerous exhibits of the critical differences in insurers' coverage, market appetite, and capacity. **You save valuable time** because *The Betterley Report* has done the groundwork for you, providing practical information in a fully searchable online format.

What do you think this dedicated research team and related market analysis is worth to you and your team? Well, you are going to be pleasantly surprised when you see how we've priced it for you.

Agents and Brokers—Sell more and grow revenue by pinpointing errors in competitors' policies/proposals.

Risk Managers and Insurance Buyers—Identify, eliminate, or avoid coverage gaps with coverage comparison charts.

Underwriters—Research competitors with quick policy comparisons.

Attorneys—Keep up with year-to-year trends in policy form development.

Consultants—Identify markets and match them up to your clients' needs.

See more benefits and read Executive Summaries of each report at **www.IRMI.com/Go/3.**

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.*

We have noted several broad trends in the Cyber insurance market and decided to dive deeper into them in this Summary and the accompanying tables:

- Insureds' concerns over Cyber exposures from attacks by state and non-state actors (i.e., state sponsored hacking for the purposes of damaging infrastructure and/or industrial espionage)
- Insureds' concerns over Cyber-based theft of Intellectual Property
- Deeper and richer value-added risk management services to help insureds avoid and cope with exposures and loss

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.

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

List of Tables

Contact and Product Information	20
Product Description	26
Market Information	36
Limits, Deductibles, Coinsurance, and Commissions	41
Data Privacy: Types of Coverage and Limits	43
Data Privacy: Coverage Provided	53
Data Privacy: Coverage Triggers	58
Data Privacy: Types of Data Covered	60
Data Privacy: Remediation Costs Covered	65
Data Privacy: Remediation Coverage Services	68
Media Liability Extensions	71
Security Assessment Requirements	77
First-party Coverage	79
State-sponsored and Terrorism Coverage	84
Theft Coverage	86
Third-Party Liability Coverage	92
Claims Reporting, ERP, Selection of Counsel, Consent to Settle	113
Prior Acts	120
Territory	122
Exclusions	124
Risk Management Services	137

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 continues to help brokers understand the exposures, coverage, and services of Cyber Risk, so that they can better serve their clients. The products are complicated, making these educational efforts are worthwhile and necessary investment.

We have tried to present a variety of coverages to illustrate what is available in the market. Twenty-eight 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-six; the two that were added have offered cyber products (and been included) in recent years. Also, Digital Risk has changed its name to Safehold Special Risk.

This year, we added coverage of Euclid Manager's dedicated cyber product; since their previous inclusion was for a product that focused on Technology E&O, we had removed that product from last year's Cyber/Privacy report. This new product focuses on Cyber, and we are glad to include it.

Liberty Specialty Markets product has been added back in, since it is a different product than the Liberty International Underwriters product that has been our sole focus recently.

We also reached out to various carriers based in Canada and Australia, but none were ready yet to participate. We expect they will be shortly, as non-U.S.-based carriers become increasingly willing to offer capacity.

Recently, cyber value-added risk management services have expanded to include personalized access to privacy experts. We asked Mike Naclerio of Enquiron (formerly the Workplace Helpline) and Jeremy Henley of ID Experts to comment on their approach.

And finally, Rick Betterley (author of this Report) offers his thoughts on the future of Cyber insurance and what needs to be done to address the broader needs of the insureds while protecting the profitability of the product. This article is entitled The Future of Cyber Insurance – We Look

Companies in This Survey

The full report includes a list of 28 markets for this coverage, along with underwriter contact information, and gives you a detailed analysis of distinctive features of each carrier's offerings. Learn more about The Betterley Report, and subscribe on IRMI.com.

Down the Road and Over the Horizon.

Please remember 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.

It could be argued that Cyber insurance is rapidly maturing, and there is some truth to that. Cyber isn't so new, at least in terms of its availability (we started writing about Cyber in 2000). But it is 'new' in terms of its recognition as a key component of most commercial insurance portfolios and in terms of its evolution of coverage wordings, which continue.

But most importantly, Cyber is 'new' in terms of the exposures being underwritten. These are evolving so rapidly that carriers are forced to continually look at their underwriting and claims management approaches. To protect themselves (and their insureds) against this rapid evolution, carriers must invest more time and attention – and especially creative attention – than they might for a product that has grown as much as Cyber has.

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 and other Intellectual Property 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.

As the small- and mid-sized (SME) insureds become a more important market opportunity, car-

riers are learning how to offer products at a lower price point. Not all insureds can afford the highest levels of protection, and perhaps don't need it (although this last point can be debated). But they do need proper protection.

Sometimes 'proper protection' includes protection that meets the requirements of the customers and clients (and sometimes their suppliers and lenders). More and more, we hear of SME's buying coverage because they are required to if they want to do business with other parties. These coverage requirements unfortunately range from the reasonable (which most insureds ought to have and are available on a commercially reason basis) to unreasonable, where the limits are much higher than can be reasonably afforded.

Worse, we are seeing business agreements that make the SME responsible for unlimited losses. These agreements ask the SME to bet their company every time they sign one of them. With no hope of securing coverage limits equal to the risk assumed, it is questionable whether the agreement should be signed.

As vendor agreements more often include requirements for Cyber insurance, we hope that they will be written with commercially-reasonable terms. These agreements are a major driver in the decision to purchase Cyber; written properly, they will make the market more efficient and healthy while still providing appropriate levels of protection.

Cyber insurance 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.

Interestingly, it seems that more of the products previously limited to liability and breach response coverages are expanding to include property (and less so, theft) product options. This to us is an indication that customer demand is increasing for these product options.

Carriers are offering Cyber Risk enhancements to existing policies, such as Business Owners, Management Liability, and other policies. These products take the form of a services-only product (no risk transfer), services plus breach response coverage, and services plus breach response plus liability. Limits are typically low and options are few, but the low additional premium can make them quite appealing to insureds. Whether they should buy these products or should consider standalone Cyber policies requires careful analysis and consideration or exposure, risk tolerance, and client/customer requirements.

We provided a much deeper discussion *Cyber Add-ons for Traditional Insurance policies* in last year's Report as well as in IRMI's The Risk Report.

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 it as a part of a Technology E&O policy) 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 may be as much as $2.0 billion (up from $1.3 billion in last year's Report).

The industry is divided by size (gross written premium) as follows:

- A limited number of very large writers, with premiums in excess of $100 million
- Several carriers in the $50-100 million range
- Several more in the $25-50 million range
- Numerous carriers and Managing General Underwriters writing $10-25 million
- Several writing in the $5-10 million and $1-5 million ranges

No carrier reported negative growth, nor did any report growth in the 1-10% range. The majority reported premium growth between 10-25%, and several reported growth of 25-50% or more.

The above information is from confidential sources and is intentionally generalized.

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. In addition, premiums have grown as insureds choose higher limits and select additional types of Cyber coverages (such as Extortion and Theft). A lot more business is being written, but at slightly lower rates and, to some extent, 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 continue at a disturbingly frequent rate. 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 eventually 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 also think that carriers will take an increasing interest in helping insureds select and

implement improved risk avoidance and mitigation techniques. This approach is similar to the property insurance approach of aiding Highly Protected Risks through rate incentives, education, broader coverage offerings, and the development and installation of protective devices.

Please see our accompanying article 'The Future of Cyber Insurance" later in this Report.

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, 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.

Pre-breach services in the past were less likely to be a compelling reason for insureds to buy Cyber policies, although excellent information and tools have been available. An exciting new trend to expand pre-breach services may provide additional reasons to buy the coverage. We think these services could alter the competitive landscape for Cyber insurers as well as improve their claims experience. As Cyber further penetrates the smaller and medium-sized account market, such services will be increasingly appealing to Insureds and valuable to insurers.

We asked carriers about the health and interest of the reinsurance market that supports Cyber Risk products, and they generally reported that reinsurers are cautiously interested in 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.

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 included more specific questions in our Private Company Management Liability Market Survey (August).

State of the Market – Trends in 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. Rates are generally flat to a bit soft, undoubtedly constrained by the great amount of competition. There are simply too many insurance companies chasing new Cyber insureds to allow much in the way of rate increases.

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 carri-

ers. 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 Deductibles

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.

We also asked about trends in deductibles and self-insured retentions – the overwhelming sentiment was to keep them as they are now.

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.

An Overview of Data Privacy Coverage

In the data security business, there is a phrase: there are organizations that have breaches and know it and there are organizations that have breaches and don't know it - yet.

We find that most prospective insureds (and their agents and brokers) are most interested in coverage for data breaches. This coverage is found (or is available) in almost all Cyber policies.

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 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
- Regulatory 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
- PCI (Credit Card) Fines and Penalties including forensic services

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
- Non-electronic 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

Are there more breaches than insurers realize? And will the prevalence of Cyber insurance make breaches more visible? We think the answer to this is yes, even though governmental breach reporting requirements have taken hold.

Remediation Coverage Services

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

Carriers often offer prepackaged and pre-negotiated 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 may 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 be offering combined property and liability programs as the demand for Business Interruption and Extra Expense coverage grows.

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.

We find that insureds are increasingly concerned about the theft of the economic value of Intellectual Property. This comes from reports, we believe, of increasing levels of industrial espionage by competitors and by governments acting in support of their economic and defense interests.

We have continued our new column to the Theft table as well as to the Exclusions 2 table to capture the insurer's coverage position regarding theft of IP. In asking the insurers about this coverage, we emphasized that it references the economic value of IP. Unfortunately, we don't think that the responses are always accurate and will continue to refine them in our Reports. Theft of the economic value of Intellectual property is a major breach exposure, and insureds need coverage.

For insureds interested in coverage for the theft of the economic value of their IP, further investigation is suggested.

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."

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 now much more 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 2014).

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

Cyber-related Risk Management services are becoming a more important product differentiator – a very positive development for the insureds, their intermediaries, and for the carriers themselves. Insureds and their advisors recognize the value that these services can bring. And carriers are becoming more convinced of their value in controlling losses. But these services have a long way to go before they reach their potential.

We have been describing the parallels in services between the Cyber insurance line and other lines, especially Employment Practices and Property (Highly Protected Risk particularly). Cyber-related Risk Management services, while helpful, have been relatively weak when compared with these other lines. This is certainly understandable for this still-relatively new line of insurance, especially considering the wide array of potential services (and potentially high cost).

To try to capture more information about the services that are available to insureds via their insurance purchase (and frankly, to encourage further development of the product), we have changed our approach in the Risk Management Services table.

This table now asks for information on the following types of services:

- Active Avoidance – which indicates whether the carrier includes products and/or services that help the insured actively protect data from breach or other covered loss (the property analogy would be sprinklers. This is intended to indicate capabilities that act independently to protect against activities that lead to breaches.
- Pre-breach Planning – services and/or tools that help the insured to prepare a contingency plan for use in the event of a breach (think of disaster recovery)
- Helpline – a staffed resource that fields questions via telephone or email (think of an EPLI helpline)
- Information Portal – a source for information and possibly tools to help in the management and response to data protection and breach

The column 'Other' allows the carrier to describe additional types of services.

Summary

Cyber/Privacy insurance products are evolving rapidly, especially in terms of market segmentation and value-added Risk Management services. Pricing remains competitive, but there is no extensive rate cutting to gain market share. Carriers are no longer pouring into the market, but instead are improving their products as they learn more about what insureds need (and desire) from their insurance purchase.

We also see carriers building out their underwriting and claims staffs to meet the needs of the many insureds and potential insureds. Underwriting discipline seems to be intact.

But there is a worrying trend - insureds are concerned about coverage for exposures beyond the criminal activity that has been the dominant exposure to date. They are worried about attacks by hostile parties such as state actors (foreign nations), non-state actors (terrorist organizations or individuals), hacktivists that seek to embarrass or damage the victimized organization, and industrial espionage that seeks to gain economic advantage via data theft, damage or disruption.

We wonder to what extent the Cyber insurance industry will be able to provide protection against such acts. Clearly war and terrorist-based claims have been difficult or impossible to insure without governmental intervention. What about these risks in the Cyber area?

* *** * * * * * * * * * * * * * * * * *

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

The Future of Cyber Insurance –

We Look Down the Road and Over the Horizon

By: Richard S. Betterley (President - Betterley Risk Consultants)

Cyber insurance is one of the fastest growing lines of insurance that we have observed in years, and certainly one of the few coverages that has attracted the attention of even the general media outlets. But that's not surprising, considering the wide range of reported breaches, the concern of most with personal privacy, and perhaps the cloak and dagger nature of the risk.

The widespread number of successful attacks against even the best run organizations has led to a huge interest in the product. Business leaders, governmental leadership, business partners, and the insurance industry have all encouraged holders of data to buy coverage. And so they are. In great numbers.

So far, insured claims have been moderate and the experience of the insurers has been favorable. Insureds and their insurance advisors are generally glad they have the coverage, hoping that they have enough limits and bought the right policy.

But I think the product is facing some major challenges that could lead to its demise, or at least retrenchment. I also think there are major opportunities that might help prevent that from happening.

Based on my 14 years of researching, writing, and especially consulting on Cyber/Privacy risk and insurance, here are some of my top-level thoughts. Hopefully the problems I note can be solved by the opportunities I describe.

Problem #1 – Too Many Breaches

One real concern is that there are so many breaches that the ability of insurance to cover the costs at a reasonable price and retention is in doubt.

We all know the unfortunate saying that there are 2 types of organizations: those that have been breached and know it, and those that have been breached and don't know about it – yet. Unfortunately, there is way too much truth in that saying. And every one of those organizations is potentially an insured.

It may be that the frequency of breaches makes the exposure uninsurable at any reasonable price and retention (at least in the eye of the insured). One insurance solution is to raise premiums and retentions to make the risk more acceptable to the insurer, but I fear that could result in many insureds choosing to go without.

This could cause the Cyber insurance line to act like flood insurance, where often only the most risky are buying insurance, and it becomes difficult to attain pricing adequacy. And insureds would lose the benefit of the claims talent and value-added risk management services offered by Cyber insurance.

Problem # 2 - The Cyber Hurricane(s)

As if Too Many Breaches isn't enough of a problem, the risk of a cyber hurricane is prominent. Such an event, where many insureds are breached through a common attack, would result in many insureds experiencing simultaneous claims.

I don't think that cyber insurers are sufficiently protected through underwriting, policy wording, or reinsurance against the risk of many insureds being breached through a common event. I hope I am wrong.

One source – but only one – of this concern is cloud computing. While cloud providers try to wall off individual customers, we understand that there are significant security challenges. One breach of a cloud provider could affect many of the customers. And many of those customers might be insured by the same carrier.

And that's not the only source of concern – common attack vectors against the same security weakness is a regular event.

So far, many of the organizations experiencing a breach are not insureds; as Cyber insurance becomes more pervasive, these attacks will result in potentially catastrophic numbers of insurance claims.

How will that carrier (or carriers) sustain large individual losses from numerous insureds that all suffer from the same common cause? There is no shared limit amongst insureds (nor would they want one) to protect the carrier.

Many Cyber insurers write relatively small numbers of insureds, which is good in one way – they won't have the large number of insureds experiencing the common breach. But in that small book of business lies a problem – relatively small amounts of total premium and relatively small staffs to handle the breach.

Larger books of Cyber insurance can perhaps control and manage the claims resulting from a cyber hurricane, but how will the smaller writers of the coverage?

This exposure is obviously ripe for a global reinsurance solution. The increasing interest in Cyber insurance evidenced by reinsurers is a hopeful sign, but still doesn't make the underlying threat of a cyber catastrophe go away. It merely spreads it.

Problem #3 – Is There Enough Underwriting and Claims Talent?

With the extraordinary rate of growth of Cyber insurance coupled with the need for skilled underwriting and claims personnel, is there enough talent available to handle it?

We see insurers engaging some very impressive staff in their cyber operations, but it takes time to become skilled at underwriting and claims. Leveraging existing seasoned staff helps, but doesn't replace the experience needed.

Compounding this problem is that the talent available is in great demand by other insurers, intermediaries (brokers, both retail and wholesale), and even vendors, such as cyber security providers. At best, this demand will only escalate salaries; at worst, the talent churn will be a drag on performance and a concern for the insurer that just lost its cyber team.

Problem #4 – Can Prices Keep Up with the Threats?

I already have mentioned my concern about 'Too Many Breaches' and 'Cyber Hurricanes' – my pricing concern relates to the ability to predict the adequate rate.

Actuaries do a wonderful job analyzing various factors, including past events, changes in exposures, societal and economic trends, and other components to help insurers set adequate rates. This job is easier (but never easy) when the historic exposures and claims are reflective of the future.

But this is far from the case with cyber – not only are the exposures recent (and until recently, poorly reported), they are hardly static. Tomorrow's cyber-attack is unlikely to be the same as yesterday's, whether we are talking about the source, the method, the target, or the result. True, there are common elements to most attacks, and these are useful in helping to predict and measure the exposure. But I would argue that they are far less useful in cyber than they are in most lines of insurance.

Without confidence in rate adequacy, insurance industry senior executives will be hard pressed to justify their continuing support of Cyber products.

Problem #5 – Cyber Policy Forms Don't Cover Several Important Exposures

When we read about the expected losses of a major victim of a cyber-attack, such as Target, we see loss estimates of $1 billion. Even for smaller targets (non-public companies, for example), losses can be huge.

But what much of the public, including many insureds, don't realize is that a Cyber insurance policy doesn't cover large components of those losses.

Depending upon the organization, the uncovered losses may include:

- Reduction in market capitalization
- Reputational losses, including damaged relationships and opportunities, both consumer and business
- Substantial business interruption and extra expense (insurable, but often at insufficient limits)
- Possible loss of the economic value of intellectual property
- Lost staff time and focus

I suspect that the perceived value of Cyber insurance will be diminished as the customer base recognizes that some of the biggest exposures are not covered.

Opportunity #1 – Cyber Insurers are Part of the Answer

I have been focusing on the risks of cyber attacks from the insurance perspective, but these concerns aren't really driven by the existence of insurance – they are driven by the attacks themselves. With or without insurance, attacks will continue to be a major problem for those who hold data. The problem doesn't go away with insurance.

But maybe (and I think definitely), Cyber insurers are a part of the solution. And perhaps in that solution are opportunities to better serve its customers and make the economy a safer place.

For the last couple of years, I have been pushing on a concept I call Cyber 3.0 or the Highly

Protected Risk or HPR approach (I am not alone in the use of the term 'HPR' for Cyber insurance). This approach involves the insurer much more in risk avoidance and mitigation, helping the insureds protect themselves against loss through more than just risk transfer.

This is an easy concept to grasp – avoid, reduce, and mitigate risk, and then where necessary transfer it to an insurer. A foundational principal of risk management.

Cyber insurers can help insureds do this, just as insurers have done for property and boiler and machinery insurance for a century – invest more in minimizing claims and spend less on claims payments.

There are a lot of companies chasing cyber security dollars; how are the insureds, especially the small- to medium-sized insureds, going to know which ones are capable, and which aren't? Who will encourage the standards that help improve cyber security services? Who will reward the insureds that are good at cyber security, and who will encourage the rest to get better at it?

I think the Cyber insurers can play an effective role in this. By doing so, they will make the product more sustainable.

Opportunity #2 – Advances in Technology Will Help

I think that there are technology advances in cyber security that will make this product more sustainable if the insureds use them. These technologies are evolving and are far from perfect, but to the extent they are effective, I think that Cyber insurance has a chance at remaining a reasonably-priced, widely available, product.

Yes, there are many claims that are less preventable by technology. The human element will always be a major source of claims, but that risk is a lot more predictable and stable than those that are driven by technology. And even those can be moderated by improved training, monitoring, and other more traditional loss control methods.

In Conclusion

Although I have a lot of concern about the future of Cyber insurance, I can also see opportunity to keep it a success. The Cyber insurance industry has a chance to ensure its future by leveraging its growing prominence at the cyber security table. That benefits the industry, the insureds, and the insurance distribution system.

And I am sure, the world as a whole.

* * * * *

Rick Betterley is the author of Cyber/Privacy Insurance Market Survey, published annually since 2000. He writes and speaks frequently on Cyber risk and insurance, as well as other specialty insurance topics. He can be reached at rbetterley@betterley.com or (978) 422-3366.

His blog, and The Betterley Report, can be found at www.betterley.com

The Virtual Privacy Expert:

One Approach to Bringing Cyber Security to the Smaller Insured

By: Mike Naclerio (President – Enquiron)
and
Jeremy Henley (Director of Breach Services – ID Experts)

Data breach and data theft have dominated the news in the last few years and, naturally, many organizations are concerned. Insurers have also noted the rise in frequency with which their insureds are experiencing data breaches. The risk is real, and not just for large businesses. Many small and mid-sized organizations are prime targets, as they are viewed (often accurately) as having weaker defenses. In fact, these organizations can be the tunnel under the defenses of the larger ultimate target.

Unfortunately, the expense and negative publicity of just one breach can ruin a business of any size, in any industry. And many organizations do not have in-house expertise to help them assess privacy risks, let alone the ability to manage data security and avoid vulnerabilities. Worse, they often don't know who to turn to for help. With this as the backdrop, ID Experts® and Enquiron™ are now offering the Virtual Privacy Expert™.

The Virtual Privacy Expert is an on-demand resource that provides online privacy tools that complement a cyber insurance policy. Offering insureds direct access to certified privacy experts, ID Experts' Breach HealthCheck® risk assessment tool, customizable privacy and security policies, and a data breach incident response plan, these tools, allow companies to proactively measure, monitor, and manage cyber liability issues ahead of a breach. Many products available today are provided after a breach occurs, which is too late. Virtual Privacy Expert is designed to get ahead of the issues and do so affordably. The Virtual Privacy Expert is easy to understand, accessible, and actionable for organizations of various sizes. Additionally, relationship mangers will provide individual client introductions to the Virtual Privacy Expert to ensure carriers realize the multifold benefits of providing the service – helping clients to get ahead of potential claims and increased client satisfaction and value recognition.

"This is a one-of-a-kind data privacy solution that includes access to certified privacy experts for advice and answers through a one-stop risk management solution. We know that the backbone of Virtual Privacy Expert's success will be the ability to reduce claims and provide quantifiable ROI to carriers and insureds," says Mike Naclerio, President of Enquiron. "Enquiron's core capabilities to guide insureds through the services, help them actively engage, and effectively utilize the Virtual Privacy Expert resources will extend affordable data privacy management to them and allow them to focus on growing their business."

Jeremy Henley, CHPC, Director of Breach Services at ID Experts adds, "We weren't interested in aggregating a list of services that a client organization could find in a number of other ways. We build something to provide real value that

companies need. In addition, we will guide them through the process to protect their data and their business."

Previous experience in the highly protected risk property insurance and Employment Practices Liability insurance lines has shown that insureds want and need direct access to experts, not just passive educational sources, to really control their risk. These services help insureds help themselves, lowering their risk of a loss and increasing the value provided by their insurance policy.

* * * * *

Mike Naclerio is the President of Enquiron – he can be reached at mnacelrio@enquiron.com or (303) 452-4571

Jeremy Henley is Director of Breach Services at ID Experts – he can be reached at jeremy.henley@idexpertscorp.com or (760) 304-4761

Like What You See in this Executive Summary?

IRMI Risk & Insurance
KnowledgeBase • Education • Community

You won't believe the value in the full reports. Now Available on **IRMI® Online** and **ReferenceConnect™**

The Betterley Report provides insightful insurer analysis on these six markets and coverage lines:

- Cyber/Privacy Insurance Market Survey
- Technology Errors & Omissions
- Employment Practices Liability Insurance
- Side A D&O Liability Insurance
- Private Company Management Liability Insurance
- Intellectual Property and Media Liability Insurance

Each annual report provides a comprehensive review (50 to 175 pages) with numerous exhibits of the critical differences in insurers' coverage, market appetite, and capacity. **You save valuable time** because *The Betterley Report* has done the groundwork for you, providing practical information in a fully searchable online format.

What do you think this dedicated research team and related market analysis is worth to you and your team? Well, you are going to be pleasantly surprised when you see how we've priced it for you.

Agents and Brokers—Sell more and grow revenue by pinpointing errors in competitors' policies/proposals.

Risk Managers and Insurance Buyers—Identify, eliminate, or avoid coverage gaps with coverage comparison charts.

Underwriters—Research competitors with quick policy comparisons.

Attorneys—Keep up with year-to-year trends in policy form development.

Consultants—Identify markets and match them up to your clients' needs.

See more benefits and read Executive Summaries of each report at **www.IRMI.com/Go/3.**

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