June 2015

BRC

THE BETTERLEY REPORT

CYBER/PRIVACY INSURANCE MARKET SURVEY—2015

For Larger Insureds, a Market in Turmoil
For the SME Insured, Eager Insurers Await

Richard S. Betterley
President
Betterley Risk Consultants, Inc.

Highlights of This Issue

- Frequent Breaches Begin To Affect the Larger Enterprise Market, Especially Retail and Health Care, with Higher Rates and Retentions Common
- Bodily Injury and Property Damage Coverage Options
- Failure To Maintain Cybersecurity Standards Exclusion Become Contentious
- Three New Carriers Added
- Bonus Commentary: Carriers Comment Anonymously on the Cybermarket Conditions for Healthcare Organizations

Next Issue

August
Private Company Management Liability Insurance Market Survey 2015

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 cyberinsurance market and decided to dive deeper into them in this summary and the accompanying tables:

- Exclusions for failure to maintain security standards
- Bodily injury and property coverage options offered
- Insureds' concerns over cyberexposures from attacks by state and non-state actors (i.e., state-sponsored hacking for the purposes of damaging infrastructure and/or industrial espionage)
- Deeper and richer value-added risk management services to help insureds avoid and cope with exposures and loss

In response to new challenges in cyber, we added the following new questions to existing tables:

- Within the table "Market Information," we added: "Is Product Primarily Targeting Insureds Based in the United States, non-United States, or Both?"
- Within the "Data Privacy: Regulatory and Statutory Coverage Provided" table, we modified a column to include whether consumer redress funds coverage was available.
- We added a new table to "Data Privacy: Payment Card Industry Coverage Provided" to ask about payment card industry (PCI) fines and penalties and whether fraud charges and/or card reissuance costs could be included.
- "Data Privacy: Remediation Costs Covered" now includes a question as to whether the costs of credit repair can be covered.
- A new table about "Third-Party Coverage: Bodily Injury and Property Damage" was added and asked about both direct and indirect coverage for each.

List of Tables

- Under "Exclusions 1," we asked whether the policy includes a failure to maintain security standards exclusion.

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 cyberrisk products; for many carriers, the same base product is used and then adapted to fit the technology service provider insured or the cyberrisk insured. Where the carrier has a separate product, we reviewed here its cyberrisk product; if it is a common base product, we included information about both.

In looking at our information, if you see that a certain insurer's policy does not include, for example, errors and omissions (E&O) coverage, keep in mind that this coverage is most important to a service provider and that the same insurer 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 cyberrisk insurers vary dramatically. Some insurers offer coverage for a wide range of exposures, while others are more limited. For the insured (or its advisers) looking for proper coverage, choosing the right product is a challenge.

Most of the insurers offer multiple cyberrisk 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, cyberrisk requires experienced risk professionals to craft the proper coverage. The insurance industry continues to help brokers understand the exposures, coverage, and services of cyberrisk, so that they can better serve their clients. The products are complicated, making these educational efforts a worthwhile and necessary investment.

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 cyberrisk insurance market.

Companies in this Survey

The full report includes a list of 31 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.

Last year's survey covered 28; the 3 that were added are ANV, Berkshire Hathaway, and Hanover.

We again reached out to various insurers 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.

Please remember that, while each insurer 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 insurers. However, the evaluation and conclusions are our own.

Rather than reproduce the insurers' exact policy wording (which of course can be voluminous), we in some cases have paraphrased their wording, in the interest of space and simplicity. Of course, the insurance policies govern the coverage provided, and the insurers 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 insurers 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,* cyberrisk coverage represents a new or recently developed form of coverage designed to address the needs of new risks confronting organizations. Cyberrisk coverage epitomizes new insurance products, presenting insurance product managers with challenges as they learn what their insureds need and what the insurers 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 insurers are forced to continually look at their underwriting and claims management approaches. To protect themselves (and their insureds) against this rapid evolution, insurers must invest more time and attention—and especially creative attention—than they might for a typical product.

Most insurers were convinced that their best opportunities are to sell cyberrisk coverage to mainstream companies that have significant cyberrisk exposures. Many of those prospective insureds are already the insurer's customers, looking for coverage not present in traditional policies. The experience of a distressingly large number of organizations both large and small in the past few years is

perhaps only the tip of the iceberg representing the threat of data and intellectual property (IP) 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, insurers 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 SMEs 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 reasonable 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 its company every time it 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 cyberinsurance, 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.

Cyberinsurance insurers have developed very different products to address what they think cyberrisk companies need; we have provided a "Product Description" table that lets the insurer 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 cyberrisk 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 insurers 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.

Insurers are offering cyberrisk enhancements to existing policies, such as businessowners, 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 stand-alone cyberpolicies requires careful analysis and consideration of exposure, risk tolerance, and client/customer requirements.

We provided a much deeper discussion, *Cyber Add-ons for Traditional Insurance policies,* in our 2013 *Report* as well as in IRMI's *The Risk Report*. Still current and worth reading.

State of the Market

The market continues to broaden, especially in health care and the SME insureds segments. Healthcare systems and their vendors in particular are buying cyberrisk (and in the case of vendors, often buying it as a part of a technology E&O policy; these premiums are not included in our growth or premium estimates below) at a rapid clip. Insurers are offering specialized products to these insureds.

In addition to health care, insurers report much of their growth coming from SME 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. cyberrisk 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 $2.75 billion (up from $2.0 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 insurers in the $50–100 million range
- Several more in the $25–50 million range
- Numerous insurers and managing general underwriters writing $10–25 million
- Several writing in the $5–10 million and $1–5 million ranges

This year, we had very good reporting by insurers, with 18 providing sufficient detail to allow us to provide good insight into market trends.

The insureds are clearly divided into the troubled-by-lots-of-breaches organizations (larger organizations as well as retail and health care) and the rest, who so far have not been experiencing the frequency of breaches. We expect the public sector to join the "troubled" group shortly if they have not already. As has been the case for years, financial institutions comprise a separate group that is underwritten separately.

Only one insurer reported negative growth; it are rethinking how it writes cyber, and this probably is the cause of the decline. It is not a major market and does not focus on larger insureds.

No insurers reported growth in the 1–10 percent range, and only two reported premium growth between 10 and 25 percent.

The big move was almost half of the reporting insurers reported growth of 26–50 percent or more.

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

Until 2015, we found that growth had been dampened by rate competition as new insurers fought for market share, and most if not all of the growth has come from new insureds. 2015 presents a different picture, with rate increases for retail and healthcare insureds increasing significantly if unevenly. Some of the desired rate increases have been partially offset by a move by the affected insureds to higher retentions

In addition, premiums have grown as insureds choose higher limits and select additional types of cybercoverages (such as extortion and theft). A lot more business is being written, but rate competition has for the most part disappeared.

We think that this market has nowhere to go but up—as long as insurers 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 insurers negotiate lower response costs and law firms get more competitive in their pricing. Higher retentions will definitely help and, in some cases, so will reduced breach response limits, as we see both increasingly being forced on retail and healthcare insureds.

Insurers are responding to the staggeringly large number of breaches by using more precise underwriting tools, offering improved risk management services, and in a few cases apparently laying off more risk to the reinsurance market. Several of our responding insurers have indicated more interest by reinsurers in supporting cyberinsurance products, a welcoming trend.

An exception to the wide and ready availability of the various cybercoverages is the portion of the policy that covers PCI fines and penalties. For insureds that are not PCI standards compliant, coverage is becoming increasingly hard to find. Even when insureds have a project under way to become compliant, insurers are reluctant to offer coverage pending completion.

In the past, insurers would allow an insured a window of time during which they could implement their compliance effort. Now, it is much more likely that the insurer will refuse to provide coverage until that effort is complete and tested.

Privacy coverage is clearly driving the market; cyberrisk seminars and conferences are packed with prospective customers, insurers, 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 cyberrisk 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 having 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 insurers 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.

We think that a strong influence on the purchase of cyberrisk insurance is the increasing awareness of the value of post-breach response coverage. We have spoken with many chief financial officers, treasurers, and risk managers who are not so sure that the case for liability protection has been made but who 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 cyberpolicies, 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 cyberinsurers as well as improve their claims experience. As cyber further penetrates the SME account market, such services will be increasingly appealing to insureds and valuable to insurers.

We asked insurers about the health and interest of the reinsurance market that supports cyberrisk products, and they generally reported that reinsurers are more interested in the product. The responding insurers reported increasing interest in cyberrisk product support. 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, a number of insurers are offering cyberrisk 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 specific cyber-related questions in our "Private Company Management Liability Market Survey" (August).

State of the Market—Trends in Rates and Retentions

We asked the insurers whether they planned rate increases (or decreases) during the upcoming year and what they expected of their competitors. As noted earlier, the market is divided into two parts: larger/retail/healthcare organizations and everyone else except financial institutions.

For the larger/retail/healthcare insured, rates are definitely rising. How much is the key question—we see a range of 5–50 percent, with the most common in the 10–25 percent band. This is for untroubled organizations; it's worse (up to 200 percent) if they have claims experience that has yet to result in significantly improved cybersecurity measures.

For the SME insured, the market is much friendlier. Rates are still competitive and renewals are generally flat, perhaps even a bit soft, undoubtedly affected by the numerous insurers getting a foothold in the cyberinsurance market. Smaller insureds tend to have lower limits and often have relatively modest claims. This will change for the worse as smaller organizations suffer breaches that result in liability claims by larger business partners and the payment card industry.

Capacity and Deductibles

Significant liability capacity exists, and higher limits can probably be stacked up if desired. Larger, retail, and healthcare insureds may have trouble finding the limits they desire, especially for breach response. Several of the insurers in this survey are willing to sit as excess over primary coverages. The entrance of Berkshire Specialty into the excess cybermarket is a welcome development.

Still, while capacity remains available, larger organizations are not able to secure the kinds of limits that they may need. This is especially true for the breach response costs, which are being severely sublimited by many insurers.

Deductibles and self-insured retentions are going up, sometimes "voluntarily" by the insured as it responds to insurer rate increases and sometimes because it is being forced on them. This makes sense to us and is probably better for the insureds in

the long term. It makes no sense for insureds to trade dollars with insurers for frequency claims.

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 cyberpolicies.

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 insurers 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 four categories:

- 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 insurers do not provide this coverage, although there can be coverage for defense costs
- PCI (credit card) fines and penalties including forensic services and card reissuance 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 insurers 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 cyberrisk insurance. (In fact, we believe that it is the primary reason why many insureds buy cyberrisk 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 insurers. It can include:

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

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.

Insurers often offer pre-packaged 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 insurer to use the services. Finally, a few of these services have a time limit for use, especially credit monitoring.

Security Assessment Requirements

Insurer-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 it does not buy the coverage. But if it does, 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 on not only the insurer's underwriting philosophy but also the nature and role of the applicant's business being considered.

Coverage

Property and Theft

The cyberinsurance industry offers property and theft (first-party) coverage and liability (third-party) coverage; some insurers offer liability only, while others offer all. We expect that more insurers 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 cyberrisk 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 still concerned about the theft of the economic value of IP. 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 IP 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

Traditionally, bodily injury and property damage losses were not covered by cyberpolicies, but insurers are beginning to change their attitude toward this.

AIG's CyberEdge PC product introduced coverage that provides bodily injury and property damage protection that may result from a cyberattack. The coverage is provided on and excess and difference-in-conditions basis (meaning the insured's other liability policies will pay first, with CyberEdge stepping in where those policies do not cover, subject of course to its own coverage terms).

Why might this be important?

- Core commercial policies are more and more often excluding cyber-related claims.
- It adds clarity in coverage for both the insured and the insured's advisers.

We think this coverage can be important and appealing to insureds and have added a new table in this *Report* asking the insurers to indicate their position for both direct and contingent bodily injury and property damage coverage available in the cyberpolicies. See the "Third-party Coverage: Bodily Injury and Property Damage" table on page 94.

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

The definition of a claim also varies significantly, with some insurers 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 cyberpolicies. As many insureds and their brokers take cyberactivities to mean "Internet" activities, accompanied by buzz about social networking, questions about coverage for libel, slander, and IP

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 cyberpolicy.

This *Report* includes a table that summarizes the (optional) media liability coverage that they might offer a cyberrisk insured. It includes information as to whether:

- coverage applies to all types of media, or is restricted to social media only, and
- IP 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 ERP wording.

Selection of counsel continues to be a delicate issue with insureds, but as we frequently see in other new lines of coverage, insurers typically reserve the right to select, or at least approve, counsel. However, some insurers 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 insurer beforehand on the counsel they want to use.

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

Specific Coverages Included in Policy

We have identified 10 specific coverages that may be, but are not always, included in a cyberrisk 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 insurers that are willing to offer the needed protections. Coverage for patent infringement, for example, is rarely (if ever) offered in basic cyberrisk forms but can be purchased from a limited number of insurers as a separate IP policy (as covered in "Intellectual Property and Media Liability Market Survey," April 2015).

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 insurer is found in the "Exclusions" table.

Note that we have added a question in "Exclusions Table 1," which asks whether the policy form

includes an exclusion for failure to maintain security standards. This is an extremely troubling exclusion, as it adds an uncertainty to the coverage.

We have spoken with several underwriters about this; our concern is that, while an insured is best served by adopting security procedures, and the insurer should consider those standards (or the failure to adopt them) in the underwriting process, it is hardly fair to the insured to make the payment of a claim contingent upon maintaining those standards.

At first, the requirement makes sense—it's good for the insured; it's reasonable for the underwriter. The problem is—what happens when the standards change, or there is a mistake and the insured is out of compliance?

For us, the exclusion is hard to accept and dangerous for the insured. An insurer may say that it never applies the exclusion, but we would not be confident that it will never be applied in the future.

We understand that warranties in the application should be enforceable. But this exclusion goes too far.

Risk Management Services

Cyber-related risk management services are an important product differentiator—a very positive development for the insureds, their intermediaries, and the insurers themselves. Insureds and their advisers recognize the value that these services can bring. And insurers 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 often commented on the parallels in services between the cyberinsurance 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 a still relatively new line of insurance, especially considering the wide array of potential services (and potentially high cost).

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 an expanded approach in the "Risk Management Services" table.

This table asks for information on the following types of services.

- Active avoidance—which indicates whether the insurer 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 e-mail (think of an employment practices liability insurance 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 insurer to describe additional types of services.

Summary

Cyber/privacy insurance is evolving rapidly in response to high demand, a high level of claims,

and an increasing level of threats. Insurers—especially those with a lot of cyber experience—are refining their underwriting tools, making increasingly valuable risk management services available to their insureds, and helping intermediaries better understand the coverages that are needed.

The market is clearly maturing, with insurers more often insisting on higher retentions for larger insureds and for insureds in retail and healthcare segments. Coverages that were formerly easy to get now require stronger security standards. (PCI is a good example.)

We see this as generally a good thing, as insurers help encourage their insureds to be better protected against loss. Better protected insureds through the positive influence of cyberinsurers will make for better claims experience, a more stable market, and a safer world.

But there is still far to go; the products too often focus on breach of private data. Coverages need to be broadened to include loss of IP, resulting bodily injury and property damage, and damage to reputation.

Some of these coverages will become more widely available, we think, as insureds better understand the actual risk and as they get better advice from their advisers.

And more complete value-added risk management services need to be made available to insureds and scaled to their size and ability to use the services and of course to the size of the premium being charged.

Insurers will struggle with filtering out the sometimes-optimistic claims of some cybersecurity providers that rightfully see the cyberinsurance business as a huge opportunity to grow their businesses. But insurers have limited budgets to provide these services, so getting it right will be vital both to the insurers and to their insureds.

We started researching cyberinsurance in 2000; little did we know that the product would be so important, so widely needed, and so fascinating. And there is more to come.

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

About The Author

Richard S. Betterley, is the president of Betterley Risk Consultants (BRC), 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 United States. It does not sell insurance or related services.

Mr. Betterley 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.

Mr. Betterley created *The Betterley Report* in 1994 to be the objective source of information about specialty insurance products. Now published six times annually, *The Betterley Report* is known for its in-depth coverage of management liability, cyberrisk, privacy, and intellectual property and media insurance products.

More recently, Mr. Betterley 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

Interesting Comments from Leading Cyber Insurers

Because of the many large enterprise data breaches that have occurred over the past year, Cyber insurers are tightening up their underwriting of larger insureds. This is nowhere more prevalent than in larger health care providers and large retailers.

In an effort to get the latest from the carriers, Rick Betterley spoke with several leading Cyber insurance product managers, asking them about the market trends for health care in particular. The specific request was for them to comment about "rate, retention, and especially contraction in response limits for larger health care institutions." The context was client renewal experiences in which the carrier would not grant sub-limits as high as expiring, was pushing hard for higher rate, and required a higher retention.

With anonymity promised, Rick was told the following:

Capacity is contracting and rates are increasing steeply for large healthcare, retail and, to some extent FI risks.

-

Sometimes these changes can be driven by a belief the risk is over insured, or it could be that the wording is broad enough that costs such as forensics and legal are part of the response costs. And those can add up. Another issue for healthcare is that HIPAA says notification has to be in writing, which most law firms read as a letter in the mail. So the alternative notification route, i.e. email, is not necessarily available. So if you had 10 million credit cards breached, you may be able to send an email to all affected individuals and pull that off for 10 cents a person give or take whereas printing and postage is probably going to run you $1 or so a person.

-

My input: primary carriers for large risks need to provide full limit to build a real tower versus the historical sub-limited approach so that the tower builds a minimal tower for the real coverage that is needed. Notification, regulatory and forensics should be full limit in national healthcare as should PCI for national retail.

-

I'm seeing premiums and retentions double for national healthcare. Also, the traditional ILFs don't work for cyber. Personally, I see this product more like cat property, which is traditionally placed on a ground up quota share basis.

-

I think that situation is highly insurer-specific based upon their experience and cyber loss ratio. We've seen new entrants come into the market and at the same time we've seen some insurers pull back on capacity.

-

It's difficult to predict overall insurer behavior. For many insurers in this marketplace their stability on a cyber book could change quickly because most have not amassed a sizable cyber book yet. The pain threshold can be rather thin before corrective actions are deemed necessary. I'd say that for many insurers your scenario would not be a typical approach. I'm not seeing that drastic a change with any regularity, it's still the anomaly. There's always the possibility that there is something regarding that particular insured that the insurer knows about and is reacting to.

For larger healthcare institutions, I do think rates are increasing and carriers will likely be more conservative with deploying larger amounts of capacity, however, reducing "responses costs" from $10 million to $2 million would likely not be the norm.

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