June 2018

THE BETTERLEY REPORT

CYBER/PRIVACY INSURANCE MARKET SURVEY—2018

Rates Slightly Softer for Some
Value-Added Risk Management Services Evolve

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

Highlights of this Issue

- The Corvus Approach to Cyber Insurance
- Chubb's Cyber Index—Using Claims Data To Help Understand Threat Sources and Trends
- MarketStance Comments on the Size of the Package Market for Cyber
- New Insurers Added: Corvus, TDC Specialty, and Validus
- Insurers Removed from Survey: Safehold and V.O. Schinnerer

Next Issue

August
Private Company Management Liability Insurance Market Survey

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 a simple release of data through the carelessness of an employee or vendor.*

We note that additional value-added risk management services are being offered, including Corvus's SmartCyber™ Dynamic Loss Prevention™ and the Chubb Cyber Index. While these are not the only insurers offering enhanced risk management services, we applaud them for their efforts to improve the security of their policyholders.

Recall 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 Errors & Omissions Market Survey."

One thing we would like to point out is the difficulty in separating technology products from cyber-risk products; for many insurers, the same base product is used, then adapted to fit the technology service provider insured or the cyber-risk insured. Where the insurer has a separate product, we reviewed 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 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 may have a separate product for those insureds. You will probably find that product reviewed in our February issue.

List of Tables

The types of coverage offered by cyber-risk insurers vary dramatically. Some 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 can be a challenge.

Most insurers 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 other 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 a worthwhile and necessary investment.

We have tried to present a variety of coverages to illustrate what is available in the market. Thirty-two sources of insurance are included in this survey. These insurers (and, in a few instances, managing general underwriters) represent the core of the cyber-risk insurance market.

Up from last year's survey of 31 insurers, we include 32 insurers: Corvus, a managing general agent (MGA) offering a tech-enabled middle-market product with noteworthy risk management features; TDC Specialties, a new market entrant focused on health care; and Validus have been added. Safehold and V.O. Schinnerer have been removed as we were unable to obtain updated information about their products.

Please remember that, while each insurer was contacted 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***.

Companies in this Survey

The full report includes a list of 32 markets for cyber/privacy insurance coverage, along with underwriter contact information, and gives you a detailed analysis of distinctive features of each carrier's offerings. For a sneak preview of the full report and all it has to offer, view the new 2018 Report Highlights.

Introduction

As with all of our market surveys, cyber-risk coverage represents a new, recently developed or rapidly evolving 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 insurers can prudently cover.

It could be argued that cyber insurance is rapidly maturing, and there is some truth to that. Cyber is not 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.

With the increasing frequency of deceptive funds transfer and extortion events, we note the following broad trends.

- Increasing interest in cyber insurance in general
- An increasing interest in coverage beyond liability and data response costs, such as crime, extortion, and business interruption/extra expense

And, of course, "traditional" concerns about loss are still a big drive for new insureds as well as renewing insureds seeking higher coverage limits.

In the earlier years of cyber-insurance products, we think most insurers were convinced that their best opportunities were to sell cyber-risk coverage to mainstream companies that have significant cyber-risk exposures. Many of those prospective insureds were already the insurer's customers, looking for coverage not present in traditional policies.

But clearly the market for cyber-insurance sales goes well beyond the original policyholders, such as banks, large healthcare providers, educators, and retail organizations. Many newer insureds come from industry sectors that were not as likely to buy cyber, although maybe they underestimated their exposure. Professional service firms, the public sector, nonprofits, and business-to-business are all frequent buyers of the coverage.

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 information technology (IT) security safeguards must be carefully considered for businesses and institutions, such as hospitals, educational institutions, and public entities.

As the small and midsize 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 small and midsize insureds 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 small and midsize insureds responsible for unlimited losses. These agreements ask the insureds 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.

Corvus, a new entrant in the cyber middle-market, appears for the first time in The Betterley Report. It uses advanced cyber-security risk management tools to help better understand the insured's risk and just as importantly to help the insured manage that risk. We think this merited a deeper dive on the Corvus approach.

Readers of this report well know our belief that tech-enabled cyber-security approaches are necessary to contain the level of risk that insurers are accepting when they provide coverage. And that insurers can provide their policyholders (and the community) with a valuable risk management benefit when they identify and engage capable cyber-security services as a part of their insurance product.

Recently, we have been looking at Corvus Insurance's Smart Cyber™, a middle-market insurance product using new data to predict and prevent cyber events that can lead to claims. Corvus is an MGA offering tech-enabled insurance products, founded by insurance industry veteran Phil Edmundson, and we are glad to include their product in this report.

Smart Cyber uses noninvasive Web scans to gather most underwriting data and requires brokers to enter minimal information for a quote. Data tools allow it to identify challenging risks making it possible to offer broader coverage and competitive premiums to those accounts that have a high Corvus score and a favorable Dynamic Loss Prevention™ report. Information on each applicant's risk score and sample recommendations for IT security improvements are available as part of the quoting process and are provided regularly to each insured during the policy year. Corvus can also analyze third-party IT security concerns allowing it to offer full policy limit contingent business interruption cyber for most insureds.

We asked Mike Karbassi, Corvus's head of Cyber Underwriting, about the cyber-security capabilities of Smart Cyber and how they help insureds, insurers, and brokers better manage their risk. After all, there are a lot of cyber-insurance products already available to middle-market insureds. Why did Corvus decide to enter cyber, and why take this approach?

Mike shared his thoughts:

> Rick, Corvus seeks not just to build a "cherry-picking" strategy that benefits Corvus by allowing us to avoid poor risks. Corvus seeks to use noninvasive Web traffic scans in order to benefit everyone in the commercial insurance

market. We bring new tools to brokers so they can help their insureds get broader coverage and lower the overall cost of risk. We help poor risks by informing them why we choose not to underwrite their accounts. We help mid- and high-scoring insureds with our ongoing Dynamic Loss Prevention™ reports that help our insureds to identify and address IT security exposures as they change during the policy year.

In most ways, this is classic risk management. That creates a win-win where our insureds are more likely to address web security threats, thereby reducing claims for them and us. To use an analog comparison, it's just like sending an inspector to a property to check on sprinkler systems; Corvus analyzes Web traffic periodically with our software tools in order to bring a competitive advantage and service to our insured. It is just a lot less expensive to build software tools to accomplish our goals than to send humans out on inspection.

Thank you, Mike. We have been using the term highly protected risk (HPR) to describe how we envision insurers might bring the very successful approach of leading property insurers to cyber. Without an HPR approach, we question whether cyber insurance can be sustainable over time. So, we are especially glad to see Corvus using an HPR approach.

Chubb has added a new source of helpful information for all organizations (not just its own policyholders) interested in better cyber security—its Chubb Cyber Index[SM]. Using data derived from its own customer base of claims, their interactive website at https://chubbcyberindex.com reports on sources of claims experienced by Chubb's cyber insureds. Data can be reviewed by type of action causing the loss, industry affected, and size of the victim (measured by revenue).

Helpfully, Chubb also comments on the types of actions that it anticipates will be leading to claims in the near future.

We applaud Chubb for sharing this information. In specialty lines, claims data is not generally publicly available; large insurers with good data enjoy a strategic advantage by having their own data and are generally loath to share it.

While Chubb is clearly not sharing its data in a way that would lessen that advantage, it has found a way to make a useful amount of data available without compromising its own interests.

Cyber insurers have developed very different products to address what they think cyber-risk 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 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 insurers offer liability-only products, while others offer a combination of property, theft, and liability coverages.

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 indicates to us that customer demand is increasing for these product options.

We are also seeing insureds becoming concerned about losses that may result from hacked invoices;

when the customer pays the invoice to the wrong party (usually because the payment instructions were altered), they blame it on the vendor (i.e., the cyber insured) and don't want to attempt recovery from their own crime insurance (and often the victim is a smaller organization that may not have proper crime coverage).

If there is a resulting lawsuit, it is true that liability coverage may apply, but who wants to require their customers to sue? Instead, a few insurers are now offering coverage for first-party losses experienced by the customers of their insureds. Others flatly refuse, and the rest are taking a watchful, waiting approach.

Insurers 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 stand-alone cyber policies requires careful analysis and consideration of exposure, risk tolerance, and client/customer requirements.

State of the Market

The market continues to broaden, especially in health care and the small to midsize insured segments. Healthcare systems and their vendors, in particular, are buying cyber insurance (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 small to midsize companies newly aware of the possibilities of liability and, especially, deceptive funds transfer cyber extortion. 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 always hard to come by, but in reviewing the market, we have concluded that the annual gross written premium may be as much as $5 billion (up from $4 billion in last year's report). Despite lower rates … amazing.

We are struck by the high growth rates of the largest writers of cyber insurance—several of the $100 million-plus insurers are seeing total premiums written increasing from annually in a range of 26–50 percent. This is a large rate of increase for a large, well-established insurer. And most of that premium is probably new insureds (with some increased limits buyers contributing new premium).

And also impressive is the next group down ($50 million–$100 million), with increases of 11–25 percent (some higher).

Keep in mind, this is in a rate environment where insureds are often seeing small rate *reductions*, not increases. So almost all of the premium increases are new sales. No wonder insurers are attracted to this line, despite its many challenges.

And also keep in mind the accelerating new premium opportunities outside the United States, especially in Europe, thanks to new and rigorous privacy standards.

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 million–$100 million range
- Several more in the $25 million–$50 million range
- Numerous insurers and managing general underwriters writing $10 million–$25 million
- Several writing in the $5 million–$10 million and $1 million–$5 million ranges

This year, we had fairly good reporting by insurers, with 11 providing sufficient details to allow us to provide reliable insight into market trends. We wish there were more.

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

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

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.

According to Insurance Services Office, Inc., MarketStance's Eric Price-Glynn, based on preliminary 2017 data released by NAIC, "package policies led the way for commercial cyber market growth in 2017. Between 2016 and 2017 premiums written on packaged policies by domestic carriers nearly doubled from $570 million to $1.1 billion—quite a remarkable development."

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 cyber-insurance products, a welcoming trend.

An exception to the ready availability of the various cyber coverages is the portion of the policy that covers payment card industry (PCI) fines and penalties. For insureds that are not compliant with PCI standards, coverage is becoming increasingly hard to find. Even when insureds have a project underway 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; cyber-risk 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 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 having an impact on the insurance market.

What might those effects 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 cyber-risk insurance is the increasing awareness of the value crime and extortion, as well as business interruption, coverages. We have spoken with many chief financial officers, treasurers, and risk managers who are now more sure that the case for liability protection has been made but that can easily see how postbreach costs and crime/extortion claims are too frequent to ignore buying coverage for.

But even this seems to be changing. The pervasiveness of breaches has made for an angry affected population and an eager plaintiffs bar. Insureds seem to be more and more concerned that this is translating into more litigation and more likelihood of a major judgment.

Prebreach 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 prebreach 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-size account markets, such services will be increasingly appealing to insureds and valuable to insurers.

Finally, as noted, there are a number of insurers 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 specific cyber-related questions in our "Private Company Management Liability Insurance Market Survey" (August).