June 2023

BRC

THE BETTERLEY REPORT

CYBER/PRIVACY INSURANCE MARKET SURVEY—2023

A Bit More Stability, but Still a Lot of Challenges

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

Highlights of this Issue

Coverage Innovation Slows as Insurers React to Claims and Pricing Challenges

Limits Cutbacks are Prevalent

Insurers Added: Allianz and At-Bay

Insurers Removed from Survey: Tokio Marine HCC

Premium Growth Continues, but Moderated

Next Issue

August 2023

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 a security breach by a hacker intent on stealing valuable data or a simple release of data through the carelessness of an employee or vendor.*

List of Tables

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 and Omissions Market Survey."

We want to point out the difficulty in separating technology products from cyber-risk products. For many insurers, the same base product is used and 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 mqy 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 offer coverage for a wide range of exposures, while others are more limited. Choosing the right product can be challenging for the insured (or its advisers) looking for proper coverage.

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 to serve their clients better. 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. The survey includes 32 sources of insurance. These insurers (and, in a few instances, managing general underwriters) represent the core of the cyber-risk insurance market.

We included 23 companies, adding Allianz (who has been in some of our earlier reports) and At-Bay. There was only 1 subtraction: Tokio Marine HCC. In addition, the Intact Information Risk and Recovery product has been discontinued, so it has been removed (the Information Technology Solutions-Complete product continues in our report).

Please remember that while each insurer was contacted to obtain this information, we 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.

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.

Companies in this Survey

The full report includes a list of 23 insurers offering cyber privacy liability insurance, along with underwriter contact information, and gives you a detailed analysis of distinctive features of each insurer's offerings.

Learn more about *The Betterley Report—Cyber/ Privacy Liability Insurance*.

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 insureds need and what the insurers can prudently cover.

Some argue that cyber insurance is rapidly maturing, and there is some truth to that. Cyber is not so new, at least regarding 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 its evolution of coverage wordings, which continues.

Most importantly, cyber is "new" regarding 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.

The rapidly increasing number of deceptive funds transfer and extortion events, combined with governmental regulations restricting the ability of victims to pay ransom demands, is of great concern. We're skeptical that the combination will allow insureds to transfer the risk much longer, possibly forcing them to go without traditional insurance solutions. Forms of self-assumption or self-insurance, perhaps using

captives, might provide some options. However, it may be that risk transfer for at least ransomware will be unavailable on any reasonable basis.

If risk transfer via insurance becomes unavailable, this would be unfortunate. While insurance may be thought to encourage ransomware attacks, we doubt that it does. Attackers are typically unaware of who carries cyber insurance (despite some data breaches that might have disclosed such information) or whether that insurance includes ransomware protections.

The loss to the insured of a ransomware lockup is severe enough that (we think) they are just as likely to pay the ransomware themselves. The availability of insurance recoveries may make the cost less painful, but the urgency to resume operations (or prevent a data release) remains.

And if insureds lose access to risk management services that help them deal with a ransomware attack, that would be unfortunate.

The prevalence of headline ransomware attacks is driving an increasing interest in cyber insurance. Of course, "traditional" concerns about loss are still a big drive for new and 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 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 range from 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. 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 healthier while still providing appropriate levels of protection.

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 various 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.

Coverages that offer property and theft product options are prevalent. The prevalence of these coverages indicates that customer demand has increased the availability of these product options.

We are also seeing insureds concerned about losses that may result from hacked invoices. An example is when the customer pays the invoice to the wrong party, usually because the payment instructions were altered. The customer will typically blame it on the vendor (i.e., the cyber insured), as the customer does not want to attempt recovery from their own crime insurance. 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.

State of the Market

The big stories for 2023 are, of course, ransomware, continuing high levels of work at home, and, sadly, the war in Ukraine.

Why are ransomware attacks increasing? And how is the pandemic involved?

- Work from home means more electronic communication and lessened opportunity (and perhaps willingness) to double-check the authenticity of attachments and instructions.
- Economic pressures mean fewer resources to protect against and respond to threats; inflation and insufficient staff are taking their toll even in cyber security.
- Increased focus on delivering goods and services online means the increased importance of online business activity, making victims more likely to pay the ransom than to fight it at the risk of losing their business.

As for market trends, we asked MarketStance for their insight into the size of the cyber-insurance market in the United States. The results of their analysis follow.

In a review of the cyber market data reported to the National Association of Insurance Commissioners (NAIC) by US-based cyber underwriters, we

noticed that in 2022 standalone cyber policies in force grew by just 2 percent, a marked decrease from the 32 percent growth seen from 2020–2021.

This decreased growth was also less than the 16 percent growth seen in direct written premiums in 2022, from $3.15 billion to $3.65 billion. As a result, premiums written per policy increased to $13,760 from $12,160, continuing an upward trend from 2020. For the broader market of standalone and packaged cyber policies, direct written premiums grew by 15 percent, from $4.83 billion to $5.59 billion.

Looking at the US market, including Lloyd's and other alien excess and surplus (E&S) writers, and the packaged and personal lines cyber security premiums, preliminary estimates from MarketStance, a Verisk Underwriting Solution, indicate that 2022 direct written premiums ranged from $7.7 billion to $8.5 billion. This figure is up from $7 billion in 2021.