June 2024

THE BETTERLEY REPORT

CYBER/PRIVACY INSURANCE MARKET SURVEY—2024

A Bit More Stability, but Still a Lot of Challenges

Richard S. Betterley
President
Betterley Risk Consultants, Inc.

Jes Alexander
Senior Research Analyst
International Risk Management Institute

Highlights of this Issue

- Growth in the Number of Tech-Forward Insurers; Travelers Acquires Corvus
- How Are Cyber Insurers Responding to Artificial Intelligence (AI) Exposures?
- Insurer Added: Mosaic
- Insurers Removed from Survey: Allianz, eFranchisorSuite, Hiscox, and Liberty Specialty Markets London
- Premium Growth Continues, and Moderate Limits Cutbacks Are Prevalent

Next Issue

August 2024

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

Contact and Product Information	19
Product Description	24
Market Information	34
Capacity, Deductibles, Coinsurance, and Agent Access	37
Data Privacy: Types of Coverage and Limits Available	39
Data Privacy: Regulatory and Statutory Coverage Provided	42
Data Privacy: Payment Card Industry Coverage Provided	44
Data Privacy: Coverage Triggers	45
Data Privacy: Types of Data Covered	46
Data Privacy: Remediation Costs Covered	48
Data Privacy: Remediation Coverage Services	50
Coverage Extensions and (Sub)Limits Available for Cyber Insureds—Media Liability	52
Product Features Related to AI Exposures	56
Security Assessment by Third-Party Requirements	57
First-Party Coverage: Direct Damage and Business Interruption	58
Coverage for Loss Resulting from a State-Sponsored Act	60
Coverage for Loss Resulting from a Non-State-Sponsored Terrorist Act	68
Theft (First-Party) Coverage	74
Theft (First-Party) Coverage—Deceptive Funds Transfer or Social Engineering	77
Third-Party Coverage: Bodily Injury and Property Damage	80
Third-Party Coverage	82
Claims Reporting, Extended Reporting Period, Selection of Counsel, Consent To Settle	96
Prior Acts	100
Coverage Territory	101
Exclusions	102
Risk Management Services	112

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.

Artificial intelligence (AI) presents new challenges for the tech industry and society as a whole. Some think it also presents challenges (and opportunities?) for cyber-insurance products.

But does it? For our thoughts, please see below, including Jes Alexander's.

And, of course, we have a new table, which presents each insurer's position on AI coverage and, importantly, risk management services. It is a single table, as at this point few insurers are including special wordings addressing AI (whether as to coverage or limitations). Many of the insurers offered vague or no response, but we are pretty sure that all responsible cyber insurers have at least an eye on the risk.

At the moment, AI largely seems to be a vector by which an attacker might create a cyber loss, as opposed to the loss itself. If this is true, then AI is

largely an underwriting question—is the applicant subject (or more subject) to a cyber loss via an AI-enabled or enhanced attack? And/or will that attack make the insured loss more costly for the insured?

It seems less likely that it is a new type of cyber loss that requires or encourages new wording. Of course, it may well be that insureds and their advisers want to see specific wording indicating that a cyber loss that was enabled or enhanced by AI tools is included in the coverage.

Over the years, we have seen many instances where insurers at first thought that some "new" source of insured losses was already included in their standard policy, only to receive requests from insureds to clarify through specific wordings. This may well be how AI enters the cyber policy and one reason why we are starting to track it.

For those of us who are intrigued by the tech-forward approach to cyber insurance, the announcement that Corvus is being acquired by Travelers is exciting. We think tech-forward is hugely relevant (and we hope effective) for both insurers and insureds.

We asked Tim Francis, the enterprise cyber lead for Travelers, for a comment on the acquisition.

Acquiring Corvus provides Travelers with an exciting opportunity. By combining what has made Corvus successful—the data, risk control services and wholesale relationships they have—with the financial power and retail distribution of Travelers, we will strengthen our position as a market leader in cyber and continue to offer cutting-edge solutions, products, and services to our customers and trading partners.

Of course, acquisition isn't the only way to bring augmented tech capabilities to a cyber-insurance product; other insurers have tech components in their approach to cyber. But buying an established tech platform is a sharp approach to this opportunity, and we expect to see more.

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.

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

Companies in this Survey

The full report includes a list of 20 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*.

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 products to illustrate what is available in the market. The survey includes 20 sources of insurance. These insurers (and, in a few instances, managing general underwriters) represent the core of the cyber-risk insurance market.

Of the 20, an impressive number (5) are from tech-forward sources. One, Corvus, was recently purchased by Travelers; we expect there will be more acquisitions as soon as insurers grow the tech-forward market.

We added one insurer: Mosaic. Three were removed because they did not respond to multiple requests for information: Allianz, Hiscox, and Liberty Specialty Markets London. Their nonresponse does not necessarily mean that they are not interested in writing cyber, although the lack of response is disappointing.

A fourth source, eFranchisorSuite, was also removed. Our interest in that market is largely because of their focus on the franchise industry, and cyber seems to only be peripheral to their core employment practices liability (EPL)/management liability products.

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.

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. And to some prospective insureds, it's still a coverage yet to be added to their insurance portfolio.

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 may 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 ransom 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, it would be unfortunate if insureds lost access to risk management services that help them deal with a ransomware attack.

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.

Will AI-based risks drive a similar interest in cyber? We doubt it (not to say that we aren't concerned about the risks that AI brings to insureds), we just aren't convinced yet that AI is a coverage need that fits into cyber, which remains largely a breach- and ransomware-driven product.

In the early years of cyber-insurance products, we think most insurers were convinced that their best opportunities were to sell cyber-risk coverage to mainstream companies with 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, 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.