October 2024

THE BETTERLEY REPORT

CYBER INSURANCE FOR HEALTHCARE MARKET SURVEY—2024

Insurers Continue To Offer Competitive Products; Risk Managers Wonder about Artificial Intelligence Coverages

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

Highlights of this Issue

- Insurers Are Still in, but Wary
- New Table Shows How Insurers Are Responding to Artificial Intelligence Coverage Threats and Coverage Needs
- Extensive Data on Market Focus, Showing Interest Level for Specific Segments of the Healthcare Industry
- 16 Insurers Included in this Survey
- Insurers Added: Mosaic
- Insurers Removed: Hiscox
- Rates? Generally Down a Bit

Next Issue

December
Employment Practices Liability Insurance Market Survey

Editor's Note: *In this issue of* The Betterley Report, *we present our seventh review and evaluation of insurance products designed to protect against the unique risks of data security for healthcare insureds. Risks include the breach of security by a hacker intent on stealing valuable patient data or a simple release of data through the carelessness of an employee or vendor. The risks also include theft of corporate information, extortion, and interruption of services.*

List of Tables

This version of The Betterley Report *is focused specifically on healthcare insureds, although it is based in part on our June "Cyber/Privacy Insurance Market Survey." There are 16 insurers that self-identified as having a significant interest in healthcare insureds included in our report (equal to 2023, with 1 new participant and 1 removed).*

Mosaic was added to our report; Hiscox was removed as they did not respond to our requests for information.

There is extensive media coverage and concern about artificial intelligence (AI) as an opportunity and a threat to society. And, of course, insureds and insurers are interested too.

When there is a new topic of concern related to our subject, we evaluate whether it is significant enough to be examined in a report. We think AI is.

So, we have added a new table to ask base-level questions about cyber from both a coverage and an underwriting perspective.

Sometimes a new topic is of immediate concern (fraudulent funds transfer is an example) and results in immediate action by some insurers, typically those with large market share. But other new topics are of the "watch and wait" variety, for which insurers will report that they are keeping an eye on it and have not altered coverage (neither adding nor limiting). AI seems to be of the latter variety.

As you can see in our new table, "Product Features Related to AI Exposures," we asked questions about specific (policy) language related to AI and as to whether specific risk management services for AI are offered. Generally,

the insurers are not yet altering the language, with a few exceptions, and none are (yet) providing focused AI-related risk management services.

We expect that insurers will, at some point (soon?), roll out AI-related wordings, but they will largely clarify rather than limit coverage. At this stage, it is rare to hear an underwriter expecting AI to be of significant enough concern to inspire limiting or broadening language. We do expect policies to start adding in clarification language, but that will largely be inspired by the marketing benefits of being able to point to the coverage rather than to describe how the coverage is included in a definition.

Why Did We Focus on Health Care?

There are a few reasons. First, many healthcare insureds are buying (or at least seeking) cyber insurance. We are regularly asked to research products designed for those insureds.

Second, some of the exposures and coverages needed by healthcare insureds are specialized. Finally, the value-added risk management services that a healthcare organization needs are specific to its industry.

Since one of the driving forces behind The Betterley Report *is to improve products by better informing insureds (and their advisers), we hope to encourage more specialized—and appropriate—products. With better information, perhaps insureds will find the products best suited to their needs.*

Unfortunately, although we expect that there will be more, there are not many healthcare-specific cyber products on the market yet. Some insurers use healthcare-specific endorsements, which seems like a good way to modify base policies that address broader cyber-exposure concerns.

In this report, we also dig much deeper into the types of organizations that the insurer is interested in (which is not practical in our broader cyber/privacy all-industry survey in June). Look at the two "Market Focus" tables in this report for more detailed information about the specific industry types and sizes of insured each insurer will consider. One table is for healthcare providers, and the second table is for managed care organizations.

*Recall that our cyber reports do not focus on coverage for technology providers, such as Internet service providers, technology consultants, and software developers. That market is reviewed in our February issue, "*Technology Errors & Omissions Market Survey*."*

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 and choosing the right product can be a challenge.

Insurers in this Survey

The full report includes a list of 16 markets for cyber insurance for healthcare, 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 Insurance for Healthcare*

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. This is especially true for healthcare insureds, who face exposures not present for most insureds, such as the breach of private healthcare information.

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, and this survey includes 16 sources of insurance. These represent the core (but not all) of the cyber-risk insurance market for healthcare insureds.

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.

This information applies to insurers' standard products, and 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 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 (maybe) 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 continues.

Cyber for healthcare insureds is somewhat newer, in that there are fewer specialized products. Most insurers try to use their standard policy wordings for healthcare exposures. However, there are signs of a trend in creating specialized wordings and risk management service offerings for the healthcare industry. Since health care is an enormous part of the economy (especially in the United States) and has its own special sources of exposure, it might benefit from having more specialized products.

Cyber is also "new" in terms of the exposures being underwritten. These are evolving so rapidly that insurers are forced to continually review 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.

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 have expanded to include extortion, property, and bodily injury liability, and especially theft/extortion product options. This indicates to us that customer demand is increasing for these coverages.

In addition to monoline products, 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 risk transfer. Limits may be low, and options fewer, but the convenience and low additional premium can make them quite appealing to insureds. Whether they should buy these products or should consider standalone cyber policies requires careful analysis and consideration of exposure, risk tolerance, and client/customer requirements.

Healthcare Market Focus of Insurers

The healthcare industry is different, and it would be wise for insurers interested in that market to keep that in mind.

In our experience, healthcare clients expect to see insurance products that are customized to their needs while utilizing terms that are common in their industry. This expectation comes in part from the prevalence of specialized medical malpractice insurers in this space as well as the insureds' involvement in industry-specific professional societies. Although from an underwriting and claims standpoint, this common wording may not alter the meaning of the coverage. However, from the insured's standpoint, it may bring a feeling that "they understand us."

Surprisingly, we have not yet seen a lot of specialized healthcare-focused wordings. We think that may eventually change as cyber insurers look to dominate certain targeted industries.

We like this idea—as cyber matures, coverages will become fine-tuned to their insureds, underwriting and claims teams will become more specialized, and (importantly) risk management services designed for the insured's industry will become more widely available.

State of the Market

The big story for 2024 is the reduced but continuing attacks via ransomware and a return to stability in rates. Cyber-healthcare insureds are not unique in experiencing numerous ransomware claims, but they have been particularly hard hit.

Why are healthcare ransomware attacks increasing?

- The uninterrupted provision of healthcare services is vital, making providers an especially vulnerable target.
- Resources are stretched thin, making prevention and recovery more challenging.

- Work from home means more electronic communication and lessened opportunity (and perhaps willingness) to double-check the authenticity of attachments and instructions (though, of course, many healthcare workers are unable to work remotely).
- Economic pressures mean fewer resources to protect against and respond to threats.

We had eight cyber-insurer responses to our questions about rate and retention trends, but we think they accurately reflect the broader market. In summary, rate direction is trending slightly down for most insureds. Remember—this does not mean that premiums are down, as they are a function of rate and exposure.

Deductibles or self-insured retentions have returned to stability, with insurers reporting that they are mostly flat.

The responses are confidential but are summarized in the table below.

Sample Insurer Responses—
Rate and Deductible Trends (All Increasing Unless Noted)

Insurer Position in the Marketplace (Healthcare Cyber Premium Volume)	Insurer Market Focus (Size of Insured)		Rate Trend		Deductible or SIR Trend
			Own Rates	Market in General	Own Rates
Large	Large	Down	Down	Flat	Flat
Medium	Medium	–10 percent	10–15 percent	–10 percent	10–15 percent
Medium	Medium	–10 percent–+5 percent	?	Flat	Flat
Medium	All	–5 percent	–10 percent	Flat	Flat
Medium	Small–medium	Flat	Down	Flat	Flat
Medium	All	Down; depends on specific industry and attachment	0–10 percent	Down to flat	Down to flat
Small	Small–medium	Flat	0–5 percent	Flat	Flat
Small	Small–medium	–5–10 percent as excess player; flat as primary	–5–10 percent as excess player; flat as primary	Flat	Flat

Like what you see in this executive summary?

By purchasing the full report, you can learn more about how 16 insurers address the changing cyber insurance for healthcare markets.

Learn more about *The Betterley Report—Cyber Insurance for Healthcare*