



THE BETTERLEY REPORT

CYBER INSURANCE FOR HEALTHCARE MARKET SURVEY—2023

A Tough Line, but Insurers Continue To Offer Competitive Products

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

Highlights of this Issue

- Insurers Are Still in, but Wary
- Extensive Data on Market Focus, Showing Interest Level for Specific Segments of the Healthcare Industry
- 16 Insurers Included in this Survey
- Insurers Added: Liberty Mutual/Ironshore
- Insurers Removed: CNA and TMHCC
- Rates? Bouncing Around, but Generally Stable
- Deductibles Remain Stable

Next Issue

December

Employment Practices Liability Insurance Market Survey

The Betterley Report

Editor’s Note: *In this issue of The Betterley Report, we present our sixth 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.

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 (down from 17 in 2022).

Liberty Mutual/Ironshore was added to our participating insurers. TMHCC and CNA were removed as they did not provide updated information.

Why Did We Focus on Health Care?

A few reasons. First, there are a lot of healthcare insureds 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. And finally, the value-added risk management services that a healthcare organization needs are specific to their 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, there are not a lot of health-care-specific cyber products on the market yet, although we expect that there will be

List of Tables

Contact and Product Information	17
Product Description	21
Market Focus—Healthcare Organizations— Types and Size of Insureds	30
Market Focus—Managed Care Organizations— Types and Size of Insureds	36
Capacity, Deductibles, Coinsurance, and Agent Access	42
Data Privacy: Types of Coverage and Limits Available	43
Data Privacy: Regulatory and Statutory Coverage Provided	45
Data Privacy: Payment Card Industry Coverage Provided	46
Data Privacy: Coverage Triggers	47
Data Privacy: Types of Data Covered	48
Data Privacy: Remediation Costs Covered	49
Data Privacy: Remediation Coverage Services	51
Coverage Extensions and (Sub)Limits Available for Cyber Insureds—Media Liability	53
Security Assessment Requirements (By a Third Party)	55
First-Party Coverage: Direct Damage and Business Interruption	56
Coverage for Loss Resulting from State-sponsored or Terrorist Act	58
Theft (First-Party) Coverage	60
Theft (First-Party) Coverage—Deceptive Funds Transfer or Social Engineering	62
Extortion/Ransomware Coverage	64
Third-party Coverage: Bodily Injury and Property Damage	68
Third-Party Coverage	69
Claims Reporting, Extended Reporting Period, Selection of Counsel, Consent to Settle	82
Prior Acts	85
Coverage Territory	86
Exclusions	87
Risk Management Services	95

more. 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.

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 16 sources of insurance are included in this survey. 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 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.

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,

Companies 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](#)

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 continue.

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. But there are signs of a trend in creating specialized wordings and risk management services 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 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.

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 stand-alone 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 2023 is the continuing attacks via ransomware but also some return to stability in rates. Cyber-healthcare insureds are not unique in experiencing increasing ransomware claims, but they have been particularly hard hit.

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*](#)