Advisen
Transforming • Insurance

2016 SURVEY OF CYBER INSURANCE MARKET TRENDS

PartnerRe

October 2016

PARTNER RE & ADVISEN

For the third year, PartnerRe has collaborated with Advisen to undertake a comprehensive survey of the evolution of the market for cyber insurance, both first- and third-party coverage, and the factors and trends impacting that evolution. In a growing market, which PartnerRe estimates to be $2.5-$3 billion in premium, the responses shed light on shifts among key drivers of demand, as well as the challenges facing insurers as they seek to meet those demands and fulfill the market potential for this evolving line of business.

SURVEY FEATURES

The 2016 survey was conducted over the summer, at a time when large commercial data breaches did not dominate the headlines, and well before the announcement in late September that 500 million records had been breached at Yahoo! Therefore the responses were not, for the most part, greatly affected by reactions to an isolated event or market distortion, but were generally rendered with consideration of long-term trends in this global market.

Of the 321 producers and underwriters who responded, 79% indicated that they place or underwrite cyber insurance coverage, which is consistent with our previous surveys conducted in 2014 and 2015.

The survey asks questions about the current state of the market and changes over time. We also compare results with previous survey findings.

SUMMARY *of* FINDINGS

Over the past three years the PartnerRe cyber insurance survey has noted some specific shifts and trends. The most marked changes over this period are:

- The growing demand for cyber insurance coverage in sectors beyond healthcare, retail, and financial institutions, such as professional services.
- Some shifts in the factors driving sales, especially as more third parties are requiring the coverage.
- The importance of first-party coverage is changing as new causes of loss emerge, such as cyber extortion and funds transfer fraud.
- Growing interest in and coverage for bodily injury and/or property damage arising from a cyber event.

For all that has changed, many of the obstacles to selling cyber coverage remain the same, particularly a lack of education about the exposures and coverage. This lack of knowledge is especially evident in small to mid-size entities, although they are just as exposed to a cyber loss as larger organizations.

In fact, Advisen data indicates a growing variation in the size of organizations vulnerable to cyber loss. Even though large organizations remain targets, they accounted for less than 20% of cyber losses in 2016. Smaller organizations, including those with less than $1 million in annual revenue, accounted for larger percentages of the losses.

Taken together, the observations from this survey suggest that cyber insurance will at some point become common coverage for all types of enterprises, and that the insurance industry has its work to do educating the market, managing the exposures, mitigating the losses, and drawing the line between cyber coverage and other types of property and liability insurance.

This report is organized a little differently from that of previous years to reflect questions that were added or modified. The report is organized as follows:

- Coverage drivers and demands
- How coverage is provided
- Carrier placement, pricing, and claims
- Covering bodily injury and property damage
- Are cyber coverage needs being met?
- Final comments

COVERAGE DRIVERS AND DEMANDS

The sale of cyber insurance, especially in the U.S., is largely driven by those entities that hold valuable personal, health, or financial data. After a few years of some large headline losses, it is no surprise that retail, financial, and healthcare entities continue to be the main buyers. Today, some cyber-risk experts note that personal health information is targeted by hackers and data thieves as much, if not more, than financial account information. Arguably, the frequency of healthcare breaches may be due to less emphasis or controls on cyber security in the sector.

The results of the survey bear out that observation, as 49% of both underwriters and producers each cited healthcare among the top three industries bringing new buyers of cyber-insurance into the market. This indicates a strong need for the coverage in that sector, the suitability of the product, and that the cyber insurance market is still not mature, even in some of the most exposed sectors.

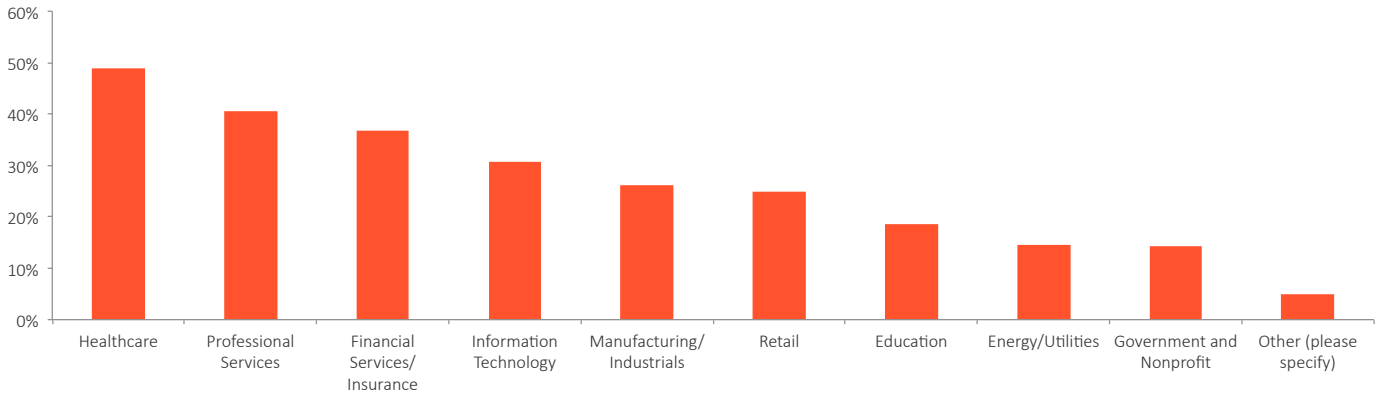
Shift in sectors that are newly buying cyber coverage

Healthcare, the leading source of new buyers, is followed by professional services, which jumped from fourth place in the 2015 survey to second this year, surpassing retail and financial services. This indicates that there is more room for growth in this new emerging sector.

Retail, which placed first in 2014 and third in the 2015 responses, dropped down to sixth among the categories of new buyers in 2016. This may reflect the higher penetration of cyber coverage in the retail sector.

Healthcare, followed by professional services, is the leading source of new buyers.

What industries bring the most NEW buyers of cyber insurance?



*Percentage total exceeds 100 as respondents could select multiple answers.

State of cyber awareness

In general, observations suggested that organizations were growing more aware of their vulnerability to cyber loss and the need to insure against it, yet underwriters and producers alike find it challenging to educate their clients and keep pace with developments in a rapidly evolving and constantly changing line.

One respondent commented that "the level of awareness of cyber risk has greatly influenced the resources dedicated to preparedness and quality of information security, in at least large organizations, and moving downstream to smaller organizations."

Another expressed a need to clarify the distinction between cyber security and cyber insurance coverage: "It's really important to provide a baseline review with clients so they understand that coverage is not a cybersecurity program, but that coverage is a funding mechanism when they have a breach."

Yet another observed that "Cyber has traditionally had a long sales cycle. By educating our sales force, and educating our customers in terms of exposures and the breadth of coverage available, the sales cycle is definitely shortening."

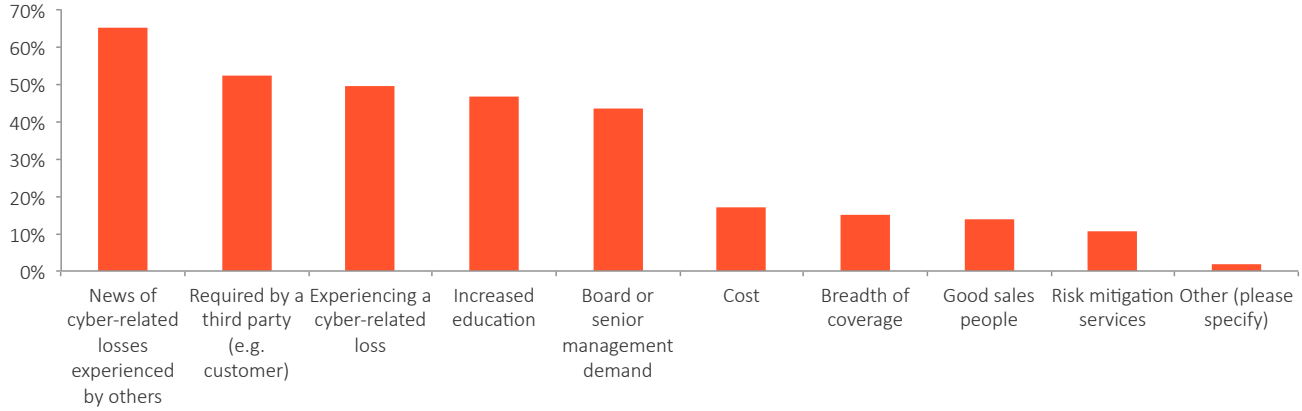
Some questioned, however, whether the realization was coming fast enough and with sufficient comprehension, as these example observations from respondents show:

- "Most clients do not feel they would be subject to a cyber-attack."
- "There is still a need to educate agents and customers regarding need, especially in small businesses."
- "There are not sufficient risk-management measures in place."
- "More and more companies are becoming aware of their companies cyber exposures and it seems to be legal, IT and risk management are working together more closely to educate the brokers and underwriters."
- "Most insureds don't understand the coverage or think they have the coverage included under their GL or Property coverage forms. Many don't understand how the coverage applies."

What drives organizations to purchase cyber coverage?

Two-thirds of respondents cited news of a cyber-related loss at another organization as a reason for a company to purchase cyber-insurance, and nearly half cited the occurrence of a cyber-related loss in the insured's own operations. Not surprisingly, these results highlight that, as losses become more prevalent, the interest in the product goes up. Interestingly, this year the requirement of cyber insurance coverage by a third party scored second highest as a buying factor, whereas last year it came fifth, marking a significant shift in entities not willing to take on any indirect exposure to cyber losses.

What do you see as the top driver of cyber product sales?



This year the requirement of cyber insurance coverage by a third party scored second highest as a buying factor.

Along with increased education regarding the exposure, substantial percentages of respondents cited requirements of board members and senior management as a driver of cyber product sales. Those factors are likely to persist long after the impact of a loss, or news of a loss, has faded.

First party coverages

As for what buyers - both new and renewal - are seeking in first-party coverage, four categories loomed large:

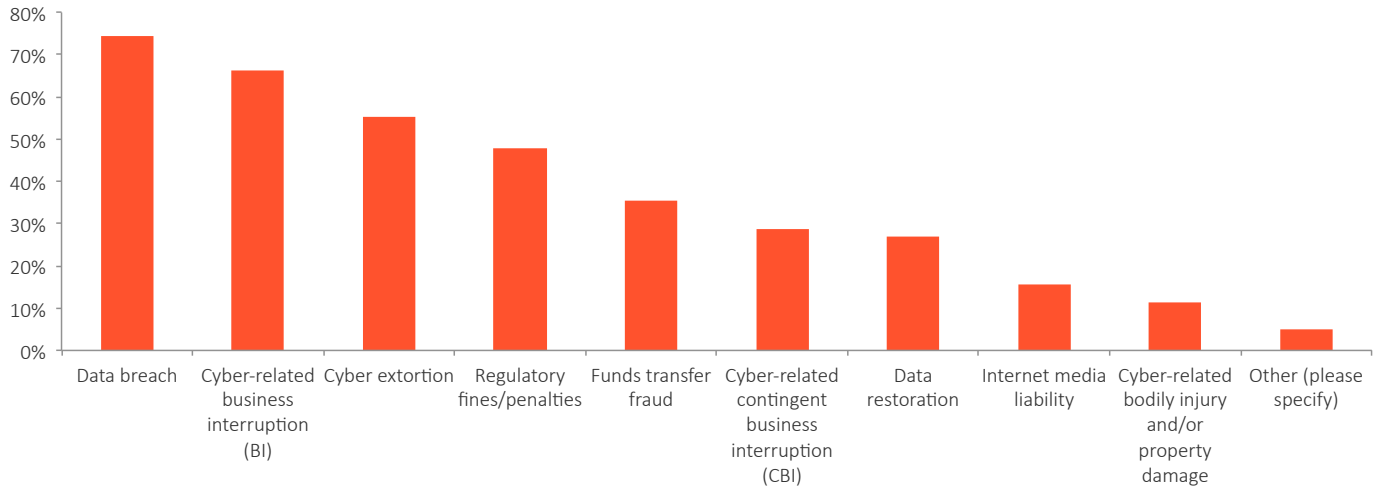
- Data breach
- Cyber-related business income
- Cyber-extortion ("ransomware")
- Regulatory fines and penalties

Even companies that do not hold data can find value in other non-data breach related coverages.

These are not surprising as data breach has long been making headlines, and over the past year, so has cyber-extortion. In fact, cyber extortion scored much higher this year than last year, where it was second to last.

With the growing offering of first party coverages, even companies that do not hold data can find value in other non-data breach related coverages, such as business interruption, cyber-extortion or funds transfer fraud coverage.

What first party cyber coverages are NEW and RENEWAL buyers most interested in purchasing?



Requested limits and available capacity

Apart from asking what kind of cyber coverage buyers wanted, the survey asked if buyers were seeking higher limits.

More than half of the respondents indicated that their clients "sometimes" seek higher limits, and a quarter of

these said their clients “frequently” seek higher limits. That’s not surprising, as the demand for the product is still maturing, losses are still being publicized, and insureds are committing more resources towards their cyber security and insurance purchase.

When asked if it has become easier to place cyber insurance towers over the past year, 88% of producers that place towers said “yes.” Given that last year 32% of producers noted that there was sometimes a capacity shortage, it appears there has been an easing on capacity constraints in the market over the past year.

Sales dynamics

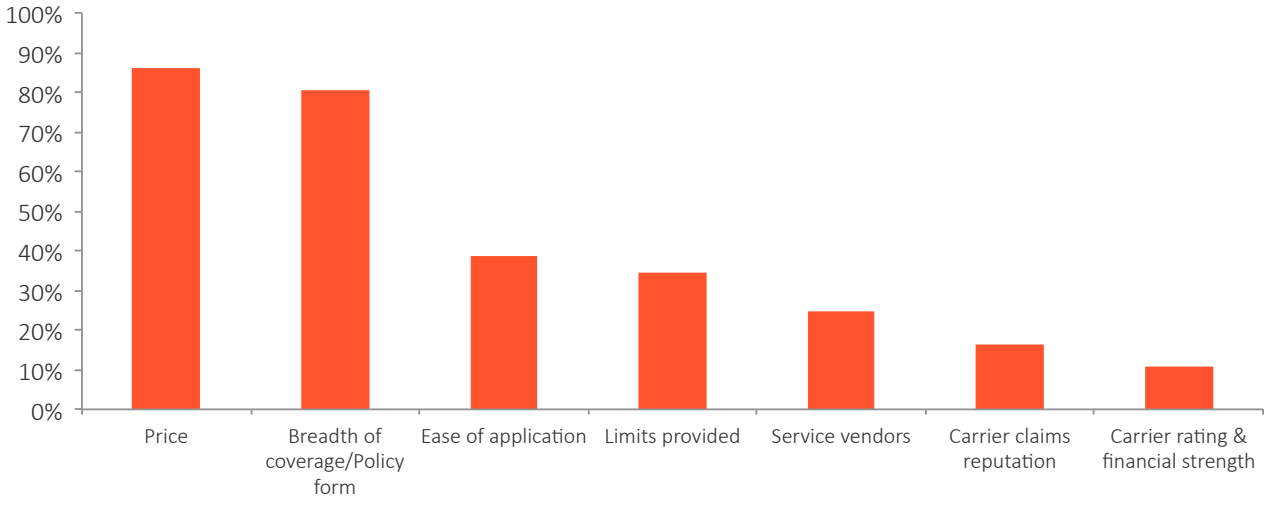
As demand for the cyber liability product grows, more producers are receiving submissions for cyber liability business.

It appears there has been an easing on capacity constraints in the market over the past year.

When asked how knowledgeable agents and brokers are in cyber risk, 89% of underwriter respondents indicated they were either “moderately” or “slightly” knowledgeable. About 3% of underwriter respondents found agents and brokers to be “extremely knowledgeable” about cyber risk. Producer knowledge is good among the majority and will continue to improve as the cyber liability product becomes more commonplace.

When asked to identify the top three factors insureds consider when making final purchasing decisions, nearly 90% of responding underwriters cited the price of coverage, which was followed by the breadth of coverage provided in the policy form. This is essentially what we found last year. Interestingly, we added “ease of application” to the answers this year, and it came in third, albeit a far third.

What are the top factors in your client’s cyber insurance buying?



Other high-ranking factors were limits provided, and service vendor support. Carrier claims reputation and carrier rating were not a significant factor in the buying decision. While the claims handling may not be a factor in the buying decision, we received several comments from producers regarding differences in claims handling among carriers which we note later on in this paper.

HOW COVERAGE IS PROVIDED

Each year, the survey has asked underwriters and producers several questions on how coverage for cyber liability is sold.

Stand-alone vs. endorsement coverage

Coverage can be provided as a stand-alone policy or as an endorsement to another policy.

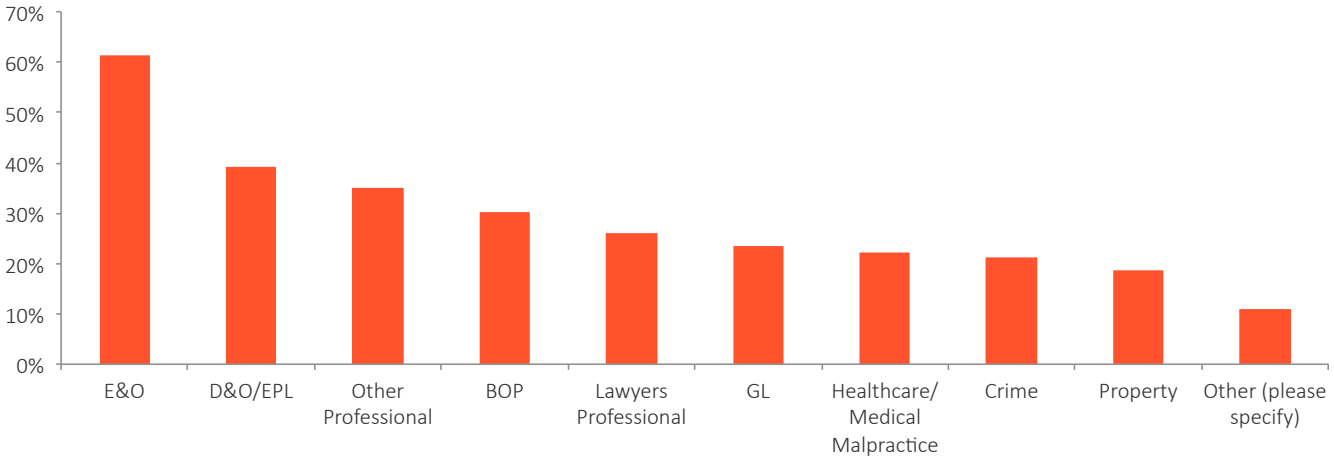
Over 60% of respondents indicated they provided the coverage through both methods. A little more than a third said they provided the coverage solely as a stand-alone policy.

Very few underwriters write cyber insurance on an endorsement basis only. This may indicate that underwriters selling endorsement coverage only may be providing the coverage on small business policies as a competitive measure.

Lines for endorsement

There are several types of policies onto which cyber coverage is endorsed, principally in lines related to professional liability.

If you write endorsements, what lines?



One respondent commented that “There is a proliferation of ‘cyber light’ coverage on BOPs which adds a false sense of security. Many businesses understand that there is a private information exposure, but not that their corporate records or physical equipment can be damaged by a cyber-attack. In fact, the word ‘cyber’ is really not consistently defined.”

"There is a proliferation of 'cyber light' coverage on BOPs which adds a false sense of security."

Another commented that: "It is very dangerous to add coverage by endorsement to package policies. The actual coverage is too limited but may appear to be broad to the buyer. The exposure is evolving constantly so policy forms need to be revised. A policy that has been renewed with the same coverage for several years is probably obsolete."

While the security of health information is a major public and private sector concern, less than a quarter of underwriters or producers indicated that they endorsed cyber coverage onto a medical professional liability. Given the high exposure of medical professionals to both medical malpractice and cyber liability claims, stand-alone cyber insurance coverage probably addresses their needs more adequately.

Inconsistent policy forms

An enduring observation of producers is that there are still substantial and persistent inconsistencies from carrier to carrier in the structure and provisions of cyber-insurance coverage forms.

There's a lot more to be done to make it easier to compare product offerings.

That said, 38% of producers surveyed indicated they think things are slowly getting better in that regard, since they responded "yes" to the question: "Is cyber insurance policy language becoming more consistent among carriers?" Still, there's a lot more to be done to make it easier to compare product offerings.

Moreover, with a few exceptions, the comments related to forms deplored the lack of consistency in them. One of the most common themes in the comments was the notable lack of consistency in terminology across policies. Other comments included:

- "Still seeing wide variations."
- "Every carrier is vastly different."
- "Will vary from market to market."
- "It is extremely difficult to do coverage comparisons."

One commenter noted that if cyber insurance were offered in a more consistent format, "it would be easier to sell."

That begs a question: Is the expansion and penetration of cyber insurance held back in any way by inconsistent forms? Or is it propelled forward by forms addressing the unique needs of insureds and risk appetites of insurers?

CARRIER PLACEMENT, PRICING, AND CLAIMS

In the eyes of producers responding to the survey, it is becoming easier to place cyber coverage, and there are fewer and fewer surprises in the pricing. As for claims handling, it remains to be seen whether significant differences will develop among carriers.

Placement and pricing

When asked how many insurance companies producers used to place primary cyber coverage, slightly more indicated "4-6" (38%) than "1-3" (36%). Beyond that, an impressive 17% indicated they placed cyber coverage with 7-10 different insurers, and another 6.6% placed coverage with 11 or more carriers.

When asked if cyber insurance pricing was becoming more consistent among carriers, slightly more than half of producers selected "yes, sometimes;" another 17% indicated "yes, frequently." Slightly less than a third chose "no, the market is very disjointed." This is an improvement over last year, when 39% of producers felt that the market was very disjointed on pricing.

One commenter noted: "Pricing often varies widely between carriers looking at the same risk. It's often surprising to markets to hear that they are not competitive on pricing, which suggests drastically different assessments of risks."

While many producers are not aware of the quality of claims handling, those that are generally note an improvement.

Claims handling

As for claims handling by carriers, the jury is still out among producers.

When asked if they noticed a difference in claims handling, 42% of responding brokers selected "don't know." But, 27% did indicate "yes." Similarly, when asked if cyber claims handling has improved, 58.8% of responding producers selected "don't know," with 29% saying "yes." So it appears that while many producers are not aware of the quality of claims handling, those that are generally note an improvement.

There were numerous comments regarding claims handling that are worth highlighting:

- "Carriers are handling claims more effectively as their claims folks gain experience and the insurance contracts become more clear."
- "Some carriers are much more proactive at the beginning of a claim. Others allow the insured more ability to handle it themselves. The right fit depends on the client."
- "Some carriers have strong in-house capabilities and relationships with outside vendors. Others outsource claims and have no existing relationships."
- "There is definitely a difference among the quality of claim services that carriers provide. Those that focus on this aspect provide a better quality of service."
- "There are more hyper-technical denials, based on claims professionals not being educated on what underwriters are selling and promising."
- "In discussions with clients and colleagues, most are sharing stories involving 'surprises over disputed claims, uncovered loss, and other issues related to cyber claims not going well'."

COVERING BODILY INJURY AND PROPERTY DAMAGE

Insureds, producers, and carriers are actively considering whether and how to provide liability coverage for bodily injury and property damage (BI/PD) resulting from a cyber-related cause of loss. Should cyber insurance policies cover BI/PD triggered by a cyber-related loss, or should other insurance policies extend their coverage to BI/PD arising from a cyber-related event?

The survey asked if insureds were inquiring about BI/PD coverage, and producer responses indicated that 40% of them found that insureds "frequently" or "sometimes" asked.

The survey went a step further and asked underwriters and producers if cyber liability coverage has been expanded to provide BI/PD coverage. Responses indicate there is some movement toward making BI/PD coverage available under cyber policies.

When producers were asked if more carriers had started offering cyber BI/PD coverage in the past year, 61% "yes, some," and another 5% indicated "yes, many."

When underwriters were asked whether their cyber policies covered BI/PD, 36% of the responding underwriters said "yes." But when those not currently offering the coverage were asked if they planned to add BI/PD coverage to their cyber products in the future, only 9% of responding underwriters said "yes;" most didn't know or answered N/A.

Comments on the general topic of cyber BI/PD coverage indicated that vocal respondents, at least, did not see a clear and compelling need for it.

- "It's provided under other policies (e.g. property, liability, etc.), no need to be part of the stand-alone cyber"
- "We write standalone cyber property damage but not in a liability policy. We may do in the future, but it often does not make sense to."
- "BI/PD are covered under GL policies already. These should be expanded to cover BI/PD caused by cyber, rather than cyber being extended to cover BI/PD."

One commenter expressed a different view, however, stating that "As claims and case law evolve, I believe there will be a significant need for BI/PD coverage due to cyber perils. Commercial product exposures are there (such as driverless cars) but the insurance market is not ready yet."

ARE CYBER COVERAGE NEEDS BEING MET?

At the end of the day, is all this working? Is cyber insurance being structured, underwritten, and marketed adequately to meet the growing exposures and needs?

An overwhelming majority of respondents, 83%, indicated that cyber insurance policies are "sometimes" meeting the needs of insureds. Another 11% indicated the policies "always" met those needs. Feedback notes that needs are being met "more now than one year ago." But respondents also noted that coverage for certain types of losses, such as social engineering fraud and intellectual property theft, needs to be expanded, and "some limits need to be higher, and not so costly."

Feedback notes that needs are being met "more now than one year ago."

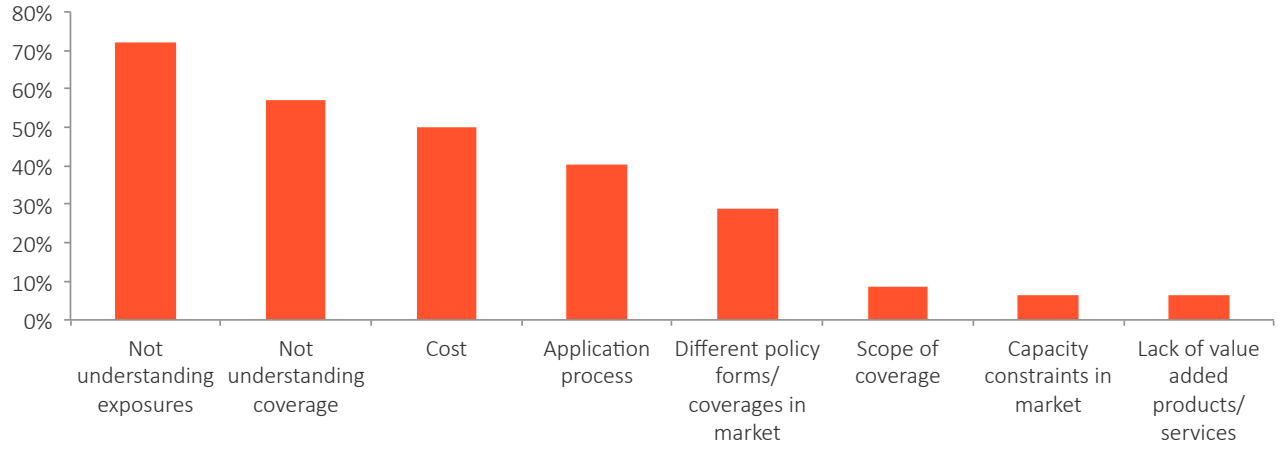
Obstacles

When underwriters and producers were asked to identify the biggest obstacles to writing cyber coverage, more than 70% of respondents cited a lack of understanding of the exposures; 57% cited a lack of understanding of the coverages.

These obstacles were followed by cost (cited by 50%), a complicated application process (40%), and variation among policy forms (28%). Far fewer underwriters cited the scope of coverage, capacity constraints, or a lack of value added products and services as obstacles.

It may be, then, that as the both the insurance industry and buyers gain better understanding of cyber exposures and coverage, forms and applications will become simplified and easier to use.

What are the biggest obstacles to selling this coverage?



"The marketplace is still growing and starting to test policies over the past couple of years," said one commenter.

Another noted that: "Cyber insurance is probably the most needed coverage of every company out there, yet it is amazing on the number of firms that feel they have no real exposure."

FINAL COMMENTS

As the cyber insurance market continues to evolve, carriers are adapting their underwriting and coverage to provide value to a wide array of insureds. It is one area of insurance where we continue to find innovation.

Cyber insurance writers will continue to react to the market needs and events, which underscores the fact that the information and results from this survey could be superseded by a market changing event that highlights an exposure or systemic problem that was not contemplated. That is the challenge in this exciting line of business.

ABOUT PARTNER RE

PartnerRe is a leading global reinsurer providing multi-line reinsurance to insurance companies for all lines of business including cyber related risk. To contact one of our cyber experts, go to partnerre.com or email christopher.mcevoy@partnerre.com in Zurich or catherine.rudow@partnerre.com in the U.S.