CYBER INSURANCE MARKET WATCH SURVEY

EXECUTIVE SUMMARY

May 2017

THE COUNCIL

The Council of Insurance Agents & Brokers

Summary

The Council of Insurance Agents & Brokers (The Council) is pleased to release its fourth biannual Cyber Insurance Market Watch Survey. The survey, which consisted of 16 questions designed to provide insights into the burgeoning cyber insurance market, creates a snapshot of the market allowing us to monitor changes and trends. Since the formation of this survey in 2015, we have seen many positive developments in the market. When it comes to purchasing cyber insurance, clients are beginning to ask the right questions as they become more familiar with the risk. We have also seen a steady increase in take-up rates among clients and prices continue to stabilize. As brokers become more experienced with cyber exposures, they are growing their knowledge of this new breed of risk and playing an increasingly crucial role in both cyber risk mitigation and post-event response.

Key Findings

Market Trends

- ✓ **32%** of respondents' clients purchased at least some form of cyber coverage
- ✓ **27%** of respondents' clients purchased cyber insurance for the first time in the past 6 months
- ✓ **44%** of respondents' clients increased their coverage in the past 6 months
- ✓ **76%** of those with cyber insurance have standalone policies

Pricing Trends

- ✓ **$6 million** is the typical cyber insurance policy limit
- ✓ **31%** of respondents said premium prices generally decreased over the last 6 months

Underwriting

- ✓ **42%** of respondents have seen some tightening of carrier underwriting practices in the last 6 months
- ✓ **75%** of respondents believe there is, for the most part, adequate clarity as to what is included and excluded in a cyber policy
- ✓ **98%** of respondents noted that capacity in the market is either plentiful or increasing

Cybersecurity/Cyber Risk

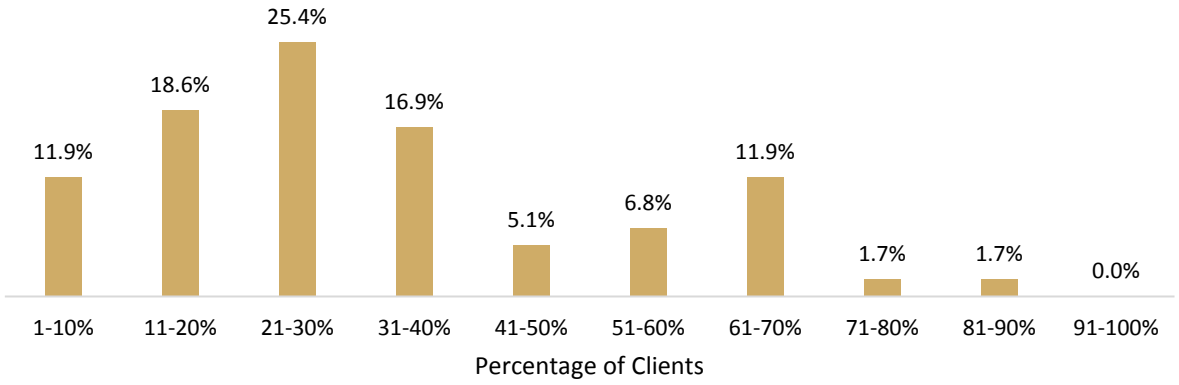
- ✓ **72%** of respondents have a strategic approach to marketing and educating clients about cyber risks
- ✓ **31%** of respondents' clients have an information security in place, focused on prevention, detection, containment and response

Survey Highlights

Take-Up

Roughly 32 percent of respondents' clients purchased some form of cyber liability and/or data breach coverage in the last six months, compared to 29 percent in October 2016 and 25 percent in April 2016. One respondent from a mid-market southeastern firm said 95 percent of their clients purchased a stand-alone cyber policy over the last six months. This increase follows a slow but steady trend, which can be contributed to several reasons: organizations of all sizes are becoming more aware of the prevalence of cyber-risks; there is better pricing with more product options; increased capacity in the market and the risk for cyber-attacks continues to increase in both volume and severity.

Roughly what percentage of your organization's clients purchase cyber liability and/or data breach coverage?



Survey respondents also suggested that the take-up rate among small and medium-sized enterprises (SMEs) is growing at a faster rate because clients are beginning to understand that cybersecurity threats affect all businesses.

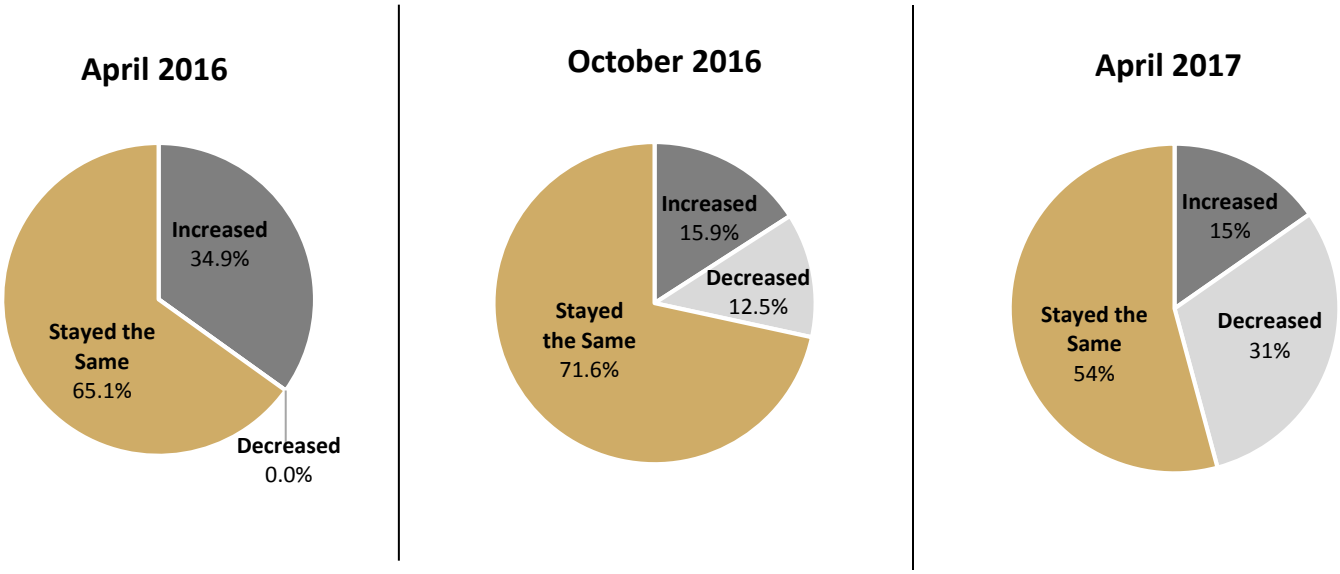
Of policyholders who purchased cyber coverage in the last six months, 44 percent increased their coverage levels while 56 maintained their existing level of coverage. Since the survey began in September 2015, no one has reported a decrease in coverage at renewal. Several respondents also said they did not have a single client decrease their coverage in the past six months. This continues to demonstrate that clients are finding value in their cyber insurance policies, in both pre-event evaluation and for post-breach response/risk mitigation. One respondent explained, "most clients that are renewing coverage are actively exploring increased limits, or at least assessing if their current limits are adequate." Another respondent noted that many contractual requirements are resulting in increased levels of coverage.

Standalone coverage over embedded coverage continued to be a trend in 2017. Roughly 72 percent of respondents' clients chose standalone over embedded coverage in the past six months and comments continued to suggest that brokers view embedded cyber coverage as inadequate. One respondent explained that embedded policies offer either "very little coverage with decent limits or pretty good coverage with extremely low limits, we do not really consider that the client has 'cyber' coverage if this is all they have."

Premium Pricing

The last six months saw trend changes in premium pricing, as 85 percent of respondents noted that premium pricing generally stayed the same or decreased. Of that 85 percent, 31 percent of respondents reported a decrease in premium pricing, compared to 12 percent in October 2016, suggesting that the market is continuing to soften. Just a year ago, nearly 40 percent of respondents reported an increase in premium pricing, proving that underwriting is tightening and policies are becoming more affordable.

Are premium prices generally increasing, decreasing or staying the same?



Limits, Capacity, Product Availability

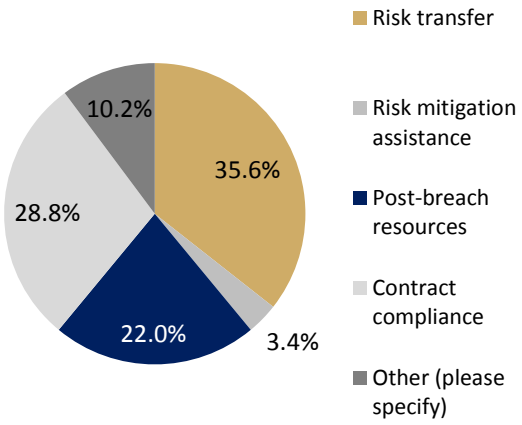
Respondents reported that the average policy limit in the last six months was around $6 million, double the reported number in October 2016 ($3 million), proving that clients are consistently increasing their limits upon renewal and clients purchasing cyber insurance for the first time are buying increased amounts of coverage. Respondents noted that it is common for clients to ask about increasing their limits or if their current policy contains enough coverage. The average largest limit placed by respondents was just over $101 million, up from $61 million six months ago. Three different respondents mentioned putting together cyber insurance towers with $600 million limits. The largest previously reported was $500 million last October.

There also remains plenty of capacity in the cyber market – 81 percent of respondents saw no capacity issues in the last six months. One respondent even described the market as “over prescribed.” While capacity in the cyber market is industry specific, as one respondent explained, capacity continues to expand in all areas, as “capital has flooded the market over the last year.” However, similar to six months ago, several respondents did note industries with higher personal and financial record counts remain tough, such as healthcare, education, retail and financial.

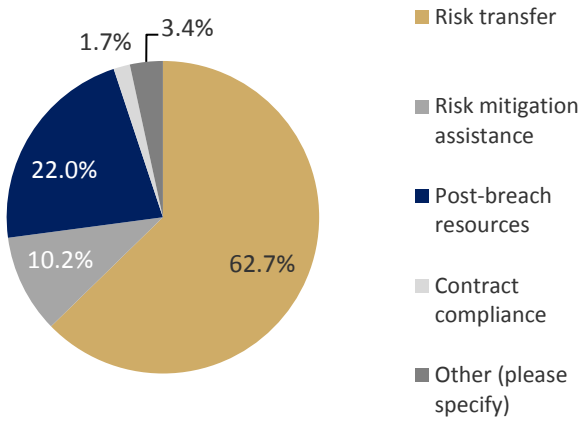
Buying Decision

When asked what drives organizations to purchase cyber insurance, risk transfer was the number one driver for large entities (63 percent) and SMEs (36 percent). For SMEs, contract compliance (29 percent) and post breach resources (22 percent) were also key factors in the purchase of cyber coverage. But many respondents noted that it is a combination of all the factors below. Overall, SMEs are beginning to realize that it no longer pertains solely to large entities, and that a cyber-event on a small organization can have crippling consequences.

What drives SMEs to purchase cyber insurance?



What drives large entities to purchase cyber insurance?



Underwriting

In the last six months, the majority of respondents (58 percent) agreed that there has not been much tightening in carrier underwriting. Higher risk classes of business: large retail, healthcare, financial institutions and fortune 500 companies continue to see increased underwriting scrutiny while underwriting for cyber insurance products aimed at SMEs remains more standardized.

Policy Language

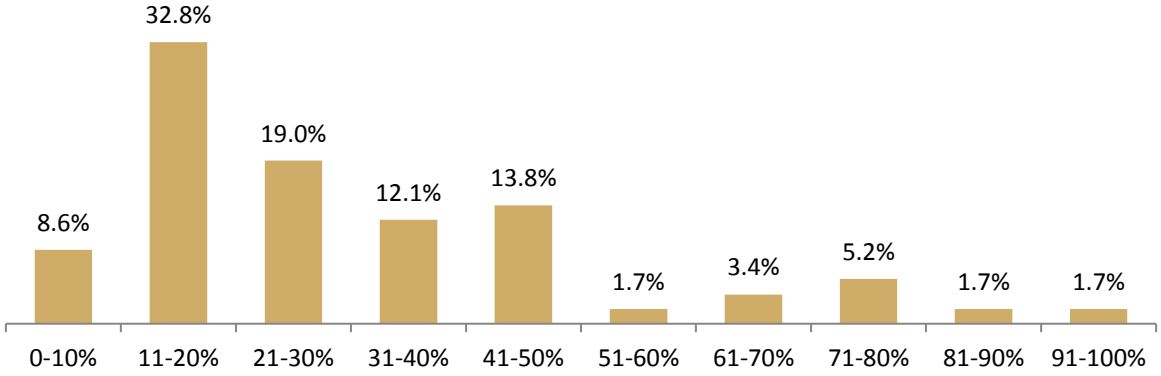
When asked if there is adequate clarity from carriers as to what is covered and excluded in a cyber policy, respondents agreed the broker needs an in-depth understanding of cyber-risks, as cyber policies are very complex and require diligent review. Many respondents explained that while policy language is “getting better,” the broker must be immersed in the product on a daily basis because there is no manuscript policy, and each carrier uses their own policy language which makes it difficult to compare coverage and terms. One broker explained, “not only is this a difficult product to understand and explain, but the carriers use different terms for the same item. Thus, just semantics is a problem in both teaching and understanding the product,” not to mention the complexities of cyber-risk in and of itself.

Education, Marketing & Risk Management

Brokers continue to be integral in educating their clients about cyber risk and their individual exposures. Seventy-two (72) percent of respondents said their firm has some sort of proactive, strategic approach to marketing and educating clients and prospects about cyber risk. Different approaches to educate this risk include: webinars, white papers, seminars, leave behinds, newsletters and modeling tools. One respondent noted that it's pivotal for the client to understand the "three aspects of client need: pre-breach auditing, post breach service and insurance coverage." Several respondents also mentioned working with strategic partners to help clients identify and quantify assets at risk.

However, organizations of all sizes are still not doing enough from a cybersecurity standpoint – only 31 percent of respondents' clients have a proactive information security program in place with capabilities in four key areas: prevention, detection, containment and response/eradication. While C-suite executives are certainly aware of this prevailing risk, entities are still struggling to allocate the proper resources and budget to adopt adequate cyber defenses.

Roughly what percentage of your clients have a proactive information security program with capabilities covering four key areas: prevention, detection, containment and response/eradication?



Strategic Partnerships

Partnerships between brokers, carriers and cybersecurity firms have been prevalent in the market. For the most part, brokers are finding these partnerships valuable in quantifying cyber-risk, but 46 percent of respondents find these partnerships valuable mainly for post-event response and consulting, not pre-event risk quantification. Thirty-seven (37) percent described the partnerships as valuable all around and 17 percent described them as not valuable. Respondents explained that these partnerships are certainly getting better, but the lack of historical data continues to be a hindrance.

Working with the Federal Government

Respondents believe there are several measures the government could implement to help create an environment in which cyber insurance is widely available and reasonably affordable. The Council's number one cyber-priority is a federal standard for reporting data breaches, and respondents echo their desire for federal legislation to move sooner rather than later. Currently, 47 unique data breach notification laws exist on the state-level creating compliance confusion.

While respondents explained that the cyber insurance market should be able to thrive on its own and that the government should "stay out of the way" when it comes to the insurance industry, many respondents agreed that tax credit on premiums, a cyber incident data repository and federal guidelines for safeguarding information systems are things the government can do to bolster the nation's cybersecurity posture and allow the cyber insurance market to thrive.

About the Survey

The Council of Insurance Agents & Brokers (The Council) represents the nation's leading insurance brokerages that collectively place 85 percent of U.S. commercial property and casualty premiums annually. During September 2015, The Council fielded its first official Cyber Insurance Market Watch Survey. The purpose of this biannual survey is to provide a retrospective snapshot of the cyber insurance market over the past six months from a nationwide sample of brokers. Brokers' insights into how their clients are—or are not—approaching cyber insurance is a unique barometer of cybersecurity in the U.S., particularly within the private sector. The thinking of many is that insurance will act as a catalyst for companies to become better at cyber risk assessment and information security in exchange for lower premiums and higher liability limits. Respondents were from a range of brokerage firms, regional agencies to the largest global brokers, wholesale and retail, whose clients range from small and medium-sized businesses to Fortune 100 companies across all industries. These brokers are on the front lines of educating clients about their tangible and intangible asset risks and coordinate insurance coverage, risk management programs, compliance and claims. The executive summary provides the highlights of the survey. The fifth Cyber Market Watch Survey will be released in October 2017. For more information on the survey, please contact Rob Boyce, The Council's Industry Affairs Associate, at Robert.Boyce@ciab.com.