CYBER INSURANCE MARKET WATCH SURVEY

EXECUTIVE SUMMARY

December 2017

THE COUNCIL

The Council of Insurance Agents & Brokers

Summary

The Council of Insurance Agents & Brokers (The Council) is pleased to release its fifth 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. "Cyber coverage is becoming an increasingly critical line of business for our members' clients," explained Ken A. Crerar, President/CEO of The Council. "However, as cybercrime continues to increase around the globe, with the average cost of a data breach approaching $4 million, it's essential for broker members to continue emphasizing the importance of adding cyber policies to clients' risk-portfolios."

Results were consistent with those in May 2017, as take-up rates remained relatively low at around 31 percent. While many clients were curious about cyber insurance, their interest did not necessarily translate to the purchase of a policy. It is interesting to note that widely publicized international events, including the Equifax breach and the WannaCry and Petya ransomware attacks, receiving international publicity, did not greatly influence adoption. Respondents also agreed that capacity remained plentiful in the market and premium pricing generally stayed the same over the last six months.

Key Findings

Market Trends

- ✓ **31%** of respondents' clients purchased at least some form of cyber coverage
- ✓ **29%** of those clients that purchased cyber insurance, 29 percent were first time buyers
- ✓ **39%** of respondents' clients increased their coverage in the past six months
- ✓ **69%** of those with cyber insurance have standalone policies

Pricing Trends

- ✓ **$5 million** is the typical cyber insurance policy limit
- ✓ **62%** of respondents said premium prices generally decreased over the last six months

Underwriting

- ✓ **66%** of respondents have not seen any tightening of carrier underwriting practices in the last six months
- ✓ **70%** of respondents believe there is, for the most part, adequate clarity as to what is included and excluded in a cyber policy
- ✓ **97%** of respondents noted that capacity in the market is either plentiful or increasing

Cybersecurity/Cyber Risk

- ✓ **87%** of respondents have a strategic approach to marketing and educating clients about cyber risks
- ✓ **34%** of respondents' clients have an information security in place, focused on prevention, detection, containment and response

Survey Highlights

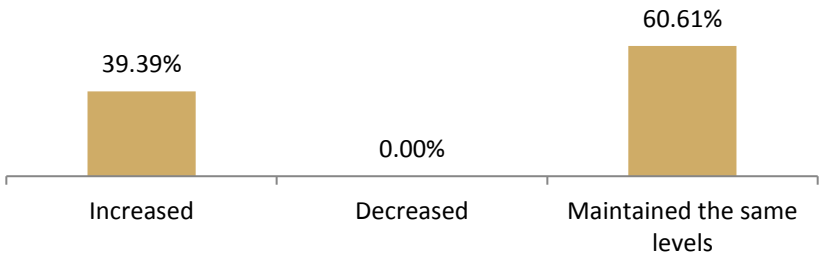
Take-Up

Approximately 31 percent of respondents' clients purchased some form of cyber liability and/or data breach coverage in the last six months, compared to 32 percent in our May 2017 survey, and 29 percent in October 2016. While take-up rates can vary drastically based on industry vertical and revenue size, overall take-up rates have been fairly consistent over the past year, according to results from the surveys. However, individual responses varied, as several noted that more of their clients are purchasing cyber insurance, and that recent events such as the Equifax breach and the WannaCry and Petya ransomware attacks have at least brought cyber coverage to the conversation.

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

Of policyholders who purchased cyber coverage in the last six months, roughly 29 percent purchased coverage for the first time. As for clients who renewed coverage, 39 percent increased their coverage levels, while 61 percent maintained their existing level of coverage. Since the survey began in September 2015, no respondent has ever reported a decrease in coverage at renewal. One respondent at a large regional Southeastern firm explained, while clients are either maintaining or increasing coverage, underwriters are also "increasing coverage with new(er) coverage extensions and little to no added premium is being charged on smaller accounts." Respondents also agreed that clients are generally becoming more interested in cyber risk and exploring whether their current limits are adequate.

Of those clients that renewed coverage in the last 6 months, did they increase coverage, decrease coverage, or maintain coverage?



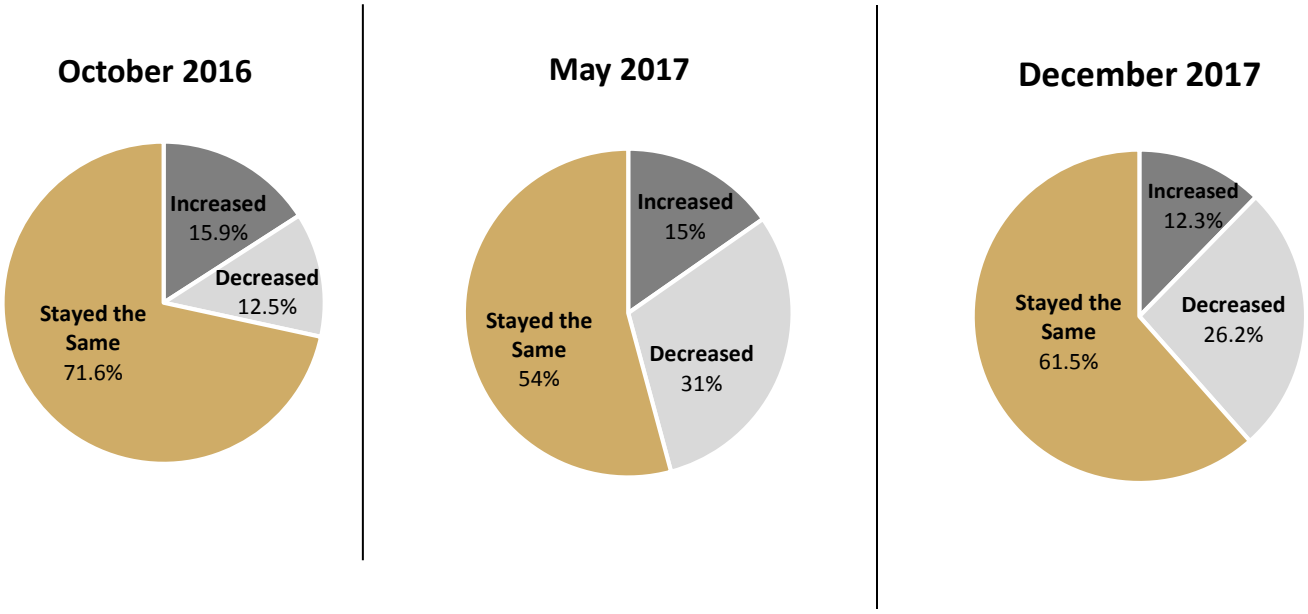
Brokers continued to stress the importance of standalone coverage over embedded coverage, explaining that embedded coverage is inadequate compared to what is available on a standalone basis. Roughly, 70 percent of respondents' clients chose standalone over embedded coverage in the past six months, also consistent with our May 2017 survey.

Premium Pricing

When asked about premium pricing over the last six months, the majority of respondents (62 percent) noted that premiums in cyber coverage generally stayed the same. Twenty-six (26) percent reported a decrease in premium pricing and just 12 percent saw an increase. Responses were in line with The Council's Q3 Property/Casualty Market Survey - premium rate change for cyber coverage was down an average of -0.7 percent in Q3 2017. Several respondents also agreed that while there are many players in the market, there are also wide variations in coverage and inconsistent pricing.

One respondent explained that renewals are staying the same on smaller business and new business is becoming more competitively priced and more easily underwritten. This 18-month trend suggests that as premium pricing continued to decrease for many clients, we have yet to see recent cyber events impact the market significantly.

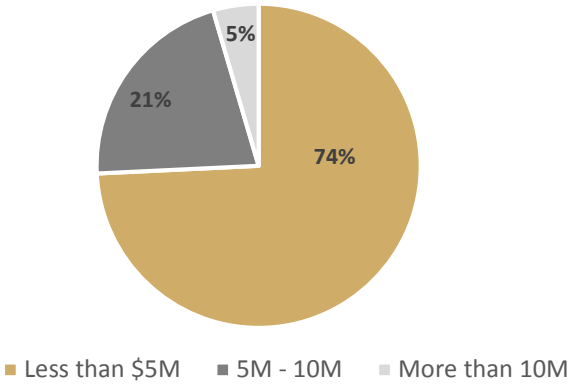
Are premium prices generally increasing, decreasing or staying the same?



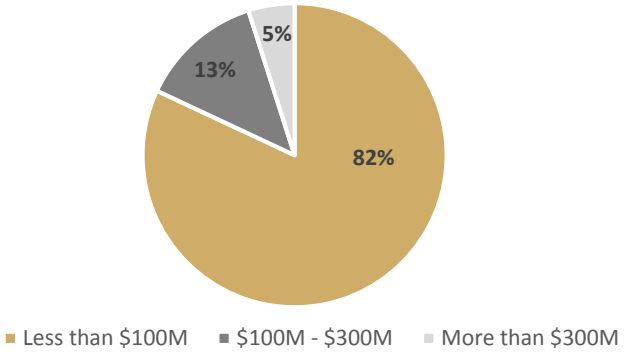
Limits, Capacity, Product Availability

The average policy limit in the last six months was around $5 million, compared to a reported $6 million average limit in May 2017, and $3 million in October 2016. Although the average policy limit is a rough estimate, the majority of respondents reported average limits of less than $5 million, which was skewed due to several reported average limits between $10-$30 million. Additionally, several respondents noted that most clients are either purchasing or considering purchasing higher limits and many added first party coverages to their cyber portfolio.

What was a typical cyber policy limit?



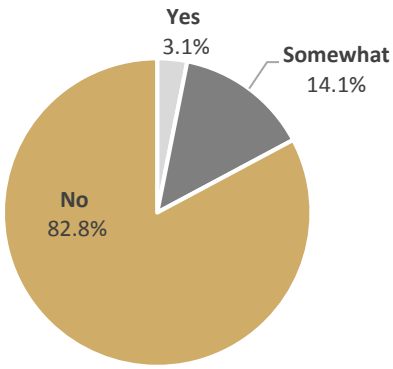
What was the largest limit you've placed?



When brokers were asked about the largest limit they have placed, responses again varied drastically, but the median response was $25 million. While the average largest limit placed in the last six months was around $170 million, it was heavily skewed by reported $300 million and $600 million towers.

Respondents agreed that capacity remains plentiful in the cyber market – 82 percent of respondents saw no capacity issues in the last six months, also consistent with results from May 2017. Several respondents noted that as capacity continues to expand, underwriting appetite appears to be broadening as well. However, industries with high financial and personal record counts, including healthcare, legal, retail and financial, continue to be tough.

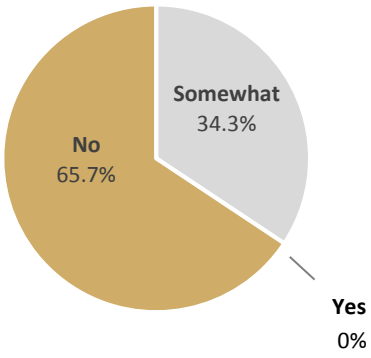
Have you seen capacity issues in the market?



Underwriting

In the last six months, brokers continued to agree that there has not been significant tightening of carrier underwriting practices. While 34 percent of respondents said there has been some increased scrutiny, no respondent believed carriers significantly increased their scrutiny of policyholder systems and procedures. Sixty-six (66) percent of those surveyed agreed that carriers have not tightened up underwriting practices, and that policies are fairly easy to place on a limited number of questions.

Did you see a significant tightening up in carrier underwriting practices

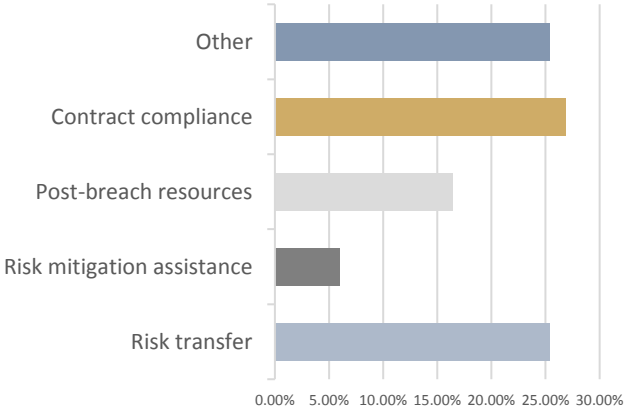


While underwriting practices in this space tend to be very industry specific, one respondent from a large Midwestern firm, saw an increase in questions around encryption and IT security environment before placing coverage. Another respondent from a midsize insurance brokerage specializing in large accounts explained that different parts of the cyber market were moving in different directions - while mature carriers have begun "maintaining controls," new carriers are lowering standards. As a result, mature carriers cannot be too stringent on underwriting due to high competition in the market.

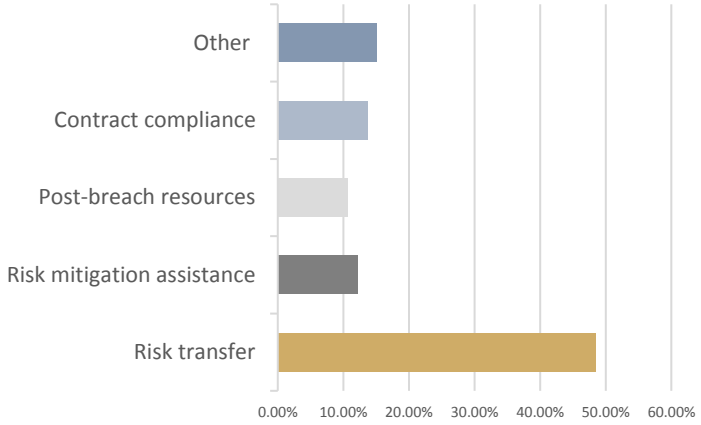
Buying Decision

When asked what drives small and medium-sized enterprises (SMEs) to purchase cyber insurance, contract compliance (27 percent) and risk transfer (26 percent) were selected by the majority. Several brokers contributed the increasing number of ransomware and malware attacks on SMEs to an uptick in cyber coverage for smaller organizations.

What motivated SMEs to purchase cyber insurance?



What motivated large entities to purchase cyber insurance in the past 6 months?

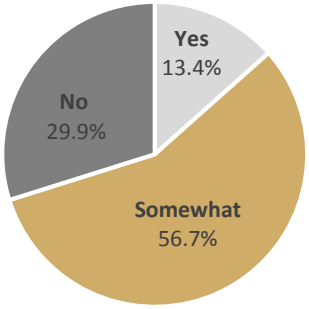


Risk transfer was again the number one driver for large entities to purchase cyber coverage in the last six months but respondents noted that all four were primary factors. One respondent explained that Boards of Directors are exhibiting more attention to cyber-risk, potentially due to the publicity around high-profile events such as the Equifax breach. The soft market, affordable pricing, availability of coverage and greater understanding of cyber-risks were also mentioned as reasons for small, medium and large entities to purchase cyber insurance.

Policy Language

When asked if there is adequate clarity from carriers as to what is covered and excluded in a cyber policy, many respondents agreed that a lack of clarity and no ISO standard make it difficult to compare policy forms. While clarity and standardization in coverage and terms is getting better, according to several respondents, each policy must be heavily scrutinized as to what is covered and what is not. Several respondents also expressed concern regarding business interruption clauses in cyber policies, explaining that they are often very difficult to settle with a client.

Is there adequate clarity from carriers as to what is covered and what is excluded in a cyber policy?



Recent Events

The second half of 2017 was one for the record books. In September, the public was notified of a March 2017 security breach on credit reporting agency, Equifax, which resulted in more than 145 million compromised records including names, birth dates, Social Security Numbers and addresses of American consumers. Additionally, the WannaCry and Petya ransomware attacks resulted in billions of dollars lost around the globe. In all, ransomware attacks are growing at a yearly rate of 350 percent with annual losses predicted to exceed $5 billion by year-end. As a result, respondents were asked how recent events changed the way organizations purchase or approach cyber coverage.

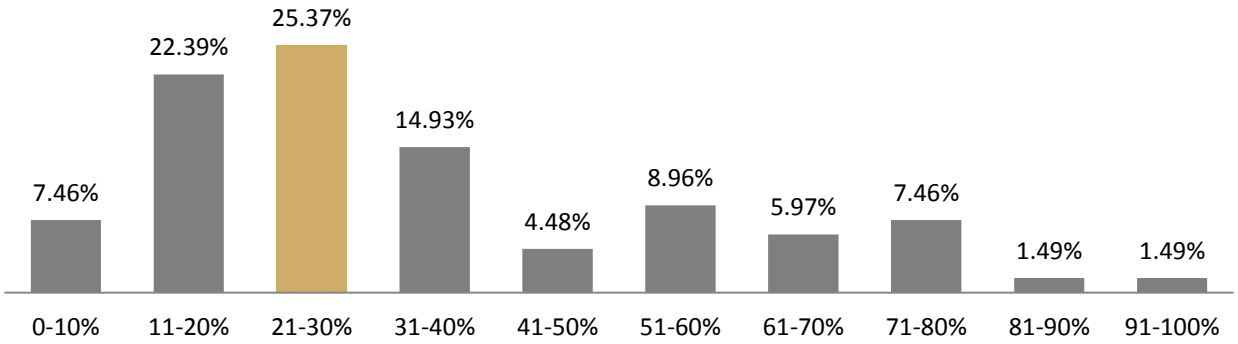
While responses varied, many brokers agreed that clients, including SMEs, are beginning to pay more attention and ask the right questions when it comes to cyber-risk. However, this did not necessarily translate to the purchase of cyber coverage, as seen in the stagnant take-up rate over the past year. Recent events have raised awareness for business interruption, one respondent explained, after reports surfaced that Petya could cost Merck and Maersk up to $300 million each. Respondents also noted that more clients are purchasing at least some minimal limits for protection, which one broker referred to as “sleep insurance.” Other respondents did not observe any change in behavior following these events, despite high publicity from the media.

Education, Marketing & Risk Management

More than 85 percent of brokers surveyed have some proactive, strategic approach to marketing and educating clients and prospects about cyber risks, a 15 percent increase from May 2017. While methods vary across firms, different approaches include webinars, seminars, white papers, risk assessment discussions, breach calculators, leave behinds and newsletters. Respondents also stressed the importance of educating their own firms on cyber risk to help their clients assess the risk and understand needed coverage levels and limits. “No matter the size of the organization, every client is presented a cyber option,” one respondent from a large national firm explained. Other firms have hired dedicated Cyber Practice Leaders or opened a specialty cyber practice, which exemplifies the investment many brokerages are making in their cyber efforts. Brokers also explained that it is important for consumers to understand the protection that cyber coverage can provide, not only from a coverage perspective, but also for pre-breach auditing and post breach services.

Brokers are also taking a mixed approach when collaborating with outside cybersecurity firms. When asked about these partnerships, the majority of respondents (62 percent) agreed that they are used for both quantifying cyber risk and post-event response. Thirty-two (32) percent said these partnerships are mainly used for post-event response and consulting. One respondent from a regional pacific firm noted an increase of exclusive programs with MGA's. While there has not been widespread collaboration among the insurance industry and cybersecurity organizations, several notable companies have recently gained traction in both risk-quantification and post-event response categories.

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



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, reasonably affordable and purchased. When asked if/what the government can do to create this environment, the majority of respondents agreed the government could play a positive role in the market, although several respondents explained 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.

Respondents were asked their thoughts on a cyber-incident data repository, a federal tax credit on cyber insurance premiums, federal guidelines for safeguarding information systems, and whether the private sector and government should share cyber threat indicators. Many respondents believed "all the above" could potentially aid the industry and most respondents selected a couple that would work best, including a national data breach reporting law. The Council's number one cyber-priority is a federal standard for reporting data breaches, and many respondents echoed that a federal standard would ease compliance burdens and confusion. Currently, 47 unique data breach notification laws exist on the state-level.

There are also several pieces of legislation that may affect Council members in some form, and noncompliance could result in heavy fines. The European Union's (EU) General Data Protection Regulation (GDPR), which comes into play on May 25, 2018, applies to all U.S. and other foreign companies that hold data of EU citizens, including insurance "intermediaries." This trailblazing legislation falls in line with Europe's stricter position on data security, but legislation in the states will follow suit – on February 15, 2018, "covered entities" including many insurance brokerages doing business in New York will be required to submit the first certification under The New York State Department of Financial Services (NYDFS) Cybersecurity Rule. Lastly, the NAIC recently adopted its Insurance Data Security Model Law, leaving it up to the states to enact and adopt the framework. If enacted by the states, brokers, carriers and other licensed entities in those states will be required by law to implement cyber security programs in accordance with the model law. For more information on cybersecurity regulation, contact The Council's General Counsel, John Fielding, at John.Fielding@ciab.com.

About the Survey

The Council of Insurance Agents & Brokers (The Council) represents the nation's leading commercial 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 sixth Cyber Market Watch Survey will be released in May 2018.

For more information on the survey, please contact Rob Boyce, The Council's Market Intelligence & Insights Associate, at Robert.Boyce@ciab.com.