CYBER INSURANCE MARKET WATCH SURVEY
EXECUTIVE SUMMARY

July 2018

THE COUNCIL

The Council of Insurance Agents & Brokers

Summary

The Council of Insurance Agents & Brokers (The Council) is pleased to release its sixth 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.

Survey results showed **no major changes over the past six months** in any of the metrics The Council tracks in comparison to the Fall 2017 survey. **Take-up rate remained low at around 32 percent**, most respondents again agreed that **market capacity was plentiful or increasing**, and **premium prices largely stayed the same**. Additionally, although many respondents said the coverage of recent cyberattacks and new regulations in the EU and the U.S. heightened awareness of cyber risks for many of their clients, that acknowledgment did not generally translate into a significant change in clients' purchasing cyber coverage.

Key Findings

Market Trends

- ✓ **32%** of respondents' clients purchased at least some form of cyber coverage
- ✓ **32%** of those clients that purchased cyber insurance were first-time buyers
- ✓ **45%** of respondents' clients increased their coverage in the past six months
- ✓ **71%** of those with cyber insurance have standalone policies

Pricing Trends

- ✓ **$3.2 million** was the typical cyber insurance policy limit
- ✓ **89%** of respondents said premium prices either stayed the same or decreased over the last six months

Underwriting

- ✓ **58%** of respondents did not see any tightening of carrier underwriting practices in the last six months
- ✓ **28%** of respondents believed there was not adequate clarity as to what is included and excluded in a cyber policy
- ✓ **78%** of respondents noted that capacity in the market is either plentiful or increasing

Cybersecurity/Cyber Risk

- ✓ **86%** of respondents' firms have a strategic approach to marketing and educating clients about cyber risks
- ✓ **34%** of respondents' clients have an information security program in place focused on prevention, detection, containment and response

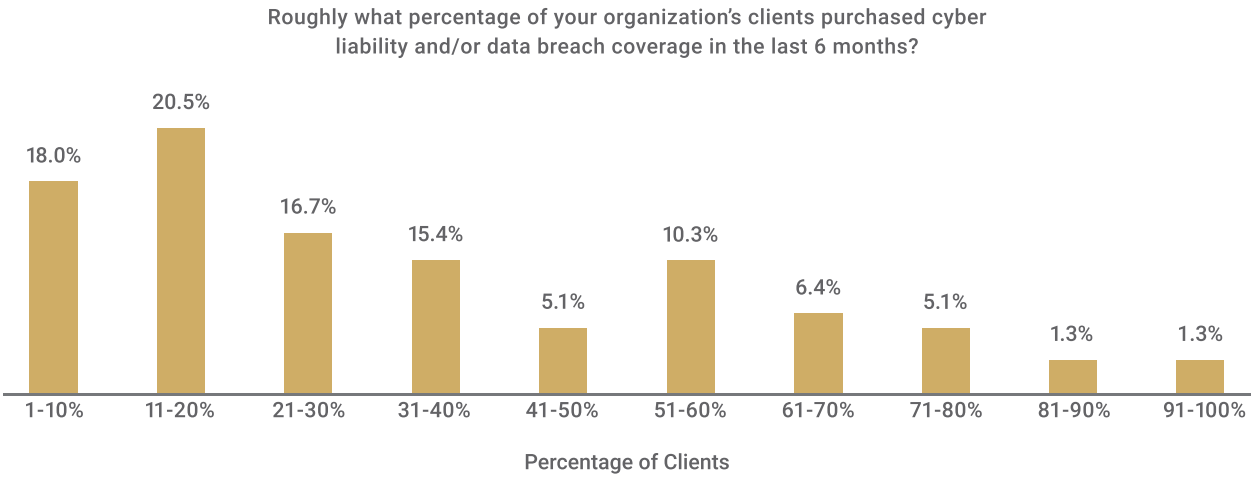
Survey Highlights

Take-Up

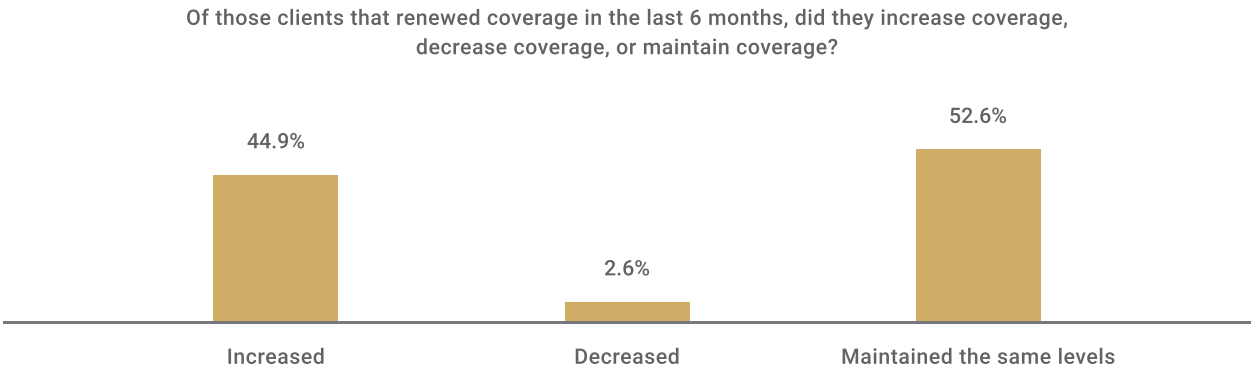
Approximately **32 percent of respondents' clients** purchased some form of cyber coverage in the past six months. This number remained consistent when compared to past surveys; respondents reported in October

2016 that 29 percent of their clients had purchased some form of cyber coverage, and that number rose slightly to 32 percent in May 2017 and 31 percent in October 2017. When respondents clarified their estimates in the comments, the numbers provided were generally in line with the weighted average of 32 percent. However, as seen in the specific graph below, some outliers affected the calculation of the average.

"Although brokers and their clients reported an increase in attention and awareness on cybersecurity and cyber coverage, we still have not seen translate to an increase in take-up rate," said Ken A Crerar, President & CEO of The Council. "Roughly 32 percent of respondents' clients purchased cyber coverage in the past six months marking no significant change over the past two years."



Of the respondents' clients who purchased cyber coverage in the past six months, **32 percent purchased it for the first time. Of those who renewed their coverage**, approximately **45 percent increased their levels of coverage**, which is a slight increase from October 2017, where it was reported that 39 percent of respondents' clients increased their coverage levels. The fact that most respondents' clients maintained or increased their coverage levels was generally supported by additional written responses: one respondent from a Northeastern firm noted that the **market was currently very competitive**, especially when it came to pricing, client retention, and coverage terms. Underwriters seemed to be trying to balance pricing discipline and appetite, said another respondent from a Midwestern firm, "but **with so many insurers, the pressure to win or retain an account was high.**"



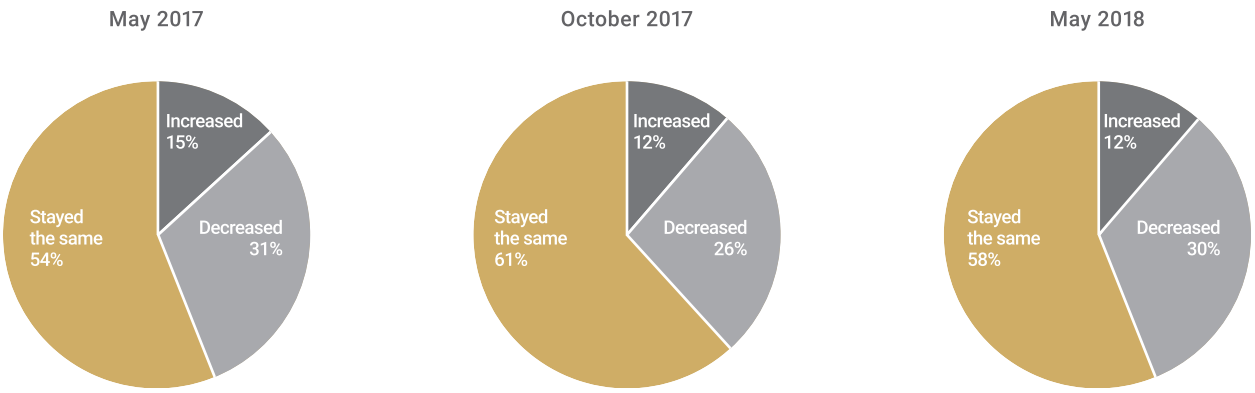
Seventy-one (71) percent of respondents' clients rely on standalone over embedded policies for cyber coverage—an increase, though marginal, from the 69 percent reported in the Fall 2017 survey. "Our push was to move towards standalone policies," one respondent explained. "We did not offer embedded cyber coverage

as an option to our clients," said another. These comments demonstrate a general trend of brokers stressing the importance of purchasing standalone over embedded policies, as embedded policies often result in coverage gaps for the client.

Premium Pricing

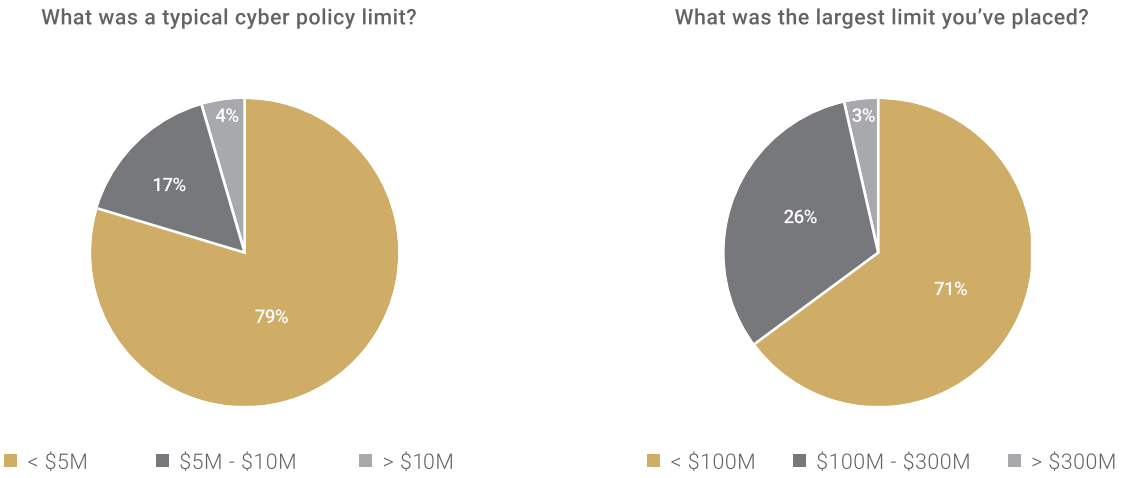
In line with previous surveys, when asked about premium pricing, **most respondents (58 percent)** indicated that premiums for cyber coverage generally stayed the same. Additionally, **30 percent of respondents** said that they had seen a decrease in premium pricing, and **just 12 percent** reported an increase. Respondents cited current market conditions as the primary factor for this trend in premium pricing, specifically noting that there was **"ample capacity" in the market**, and that competition was driving firms to lower premium rates to attract new business. This suggested that the cyber insurance market remained soft. Additionally, according to one respondent, the EU's General Data Protection Regulation (GDPR) and the New York Department of Financial Services (NYDFS) Cybersecurity Rule triggered an "enormous amount of discussion and quite a bit of purchasing," according to one respondent.

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



Limits, Capacity, Product Availability

The average policy limit over the last six months, as reported by survey respondents, was approximately $3.2 million. This was a **decrease** compared to the $5 million average policy limit in Fall 2017. While the average policy limit has been historically skewed by several larger policy limits ranging from $10 million to $50 million, **nearly 80 percent of respondents reported typical limits of less than $5 million**.

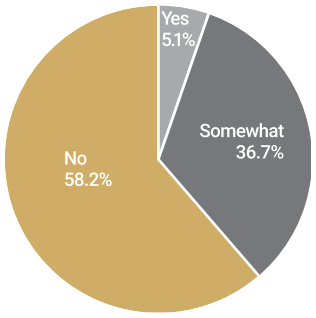


The average largest limit placed by brokers in the past six months was approximately $75 million. Although responses ranged from $1 million to $600 million, **71 percent of respondents reported largest limits of less than $100 million and 26 percent gave limits that fell between $100 million and $300 million**, up from 13 percent in the Fall 2017 survey. The $600 million tower, reported by two different firms, was a clear outlier, and heavily skewed the average $75 million limit. Lastly, many respondents agreed that the market "remained extremely competitive," and "insurers were reducing premiums and retentions if pushed with competition. Coverage terms also continued to expand."

Underwriting

In the six months since the previous survey was administered, **a majority of respondents (58 percent) reported that carriers did not increase scrutiny at all** and there was a slight increase in the percentage of respondents who reported seeing somewhat increased scrutiny in underwriting. Similar to previous surveys, an extremely small number of respondents (5 percent) believed there had been a significant tightening in carrier underwriting practices, up from 0 percent in the previous survey.

Did you see any significant tightening up in carrier underwriting practices?

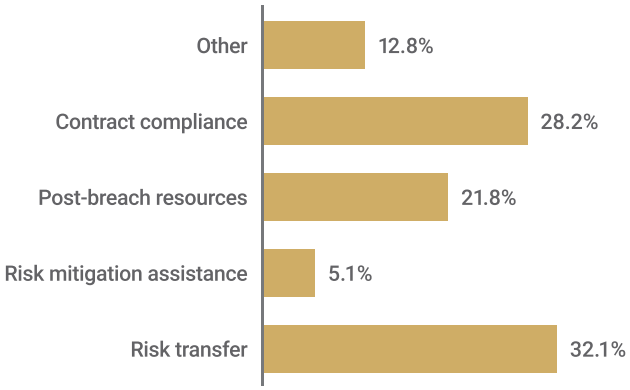


A respondent from a large Northwestern firm, who noted she had not seen a significant tightening, elaborated on her response, saying that it "depends… In areas of business interruption [there were] more questions. Elsewhere, less questions." On the other hand, **another respondent from a large national firm, who had seen increased scrutiny from carriers, explained that although there was increased** scrutiny**, it was "still easy to get coverage**," in line with the general agreement amongst respondents that the cyber market was still soft and there were "a lot of carriers entering this market space."

Buying Decision

As with the October 2017 survey, the two main factors motivating small and medium-sized enterprises (SMEs) to purchase cyber insurance were contract compliance and risk transfer: **28 percent of respondents** chose the former, and **32 percent** the latter. **GDPR compliance, growing awareness of cyber risk, and the "relatively low price"** were also cited by brokers as reasons why SMEs purchased cyber insurance.

What motivated SMEs to purchase cyber insurance in the past 6 months



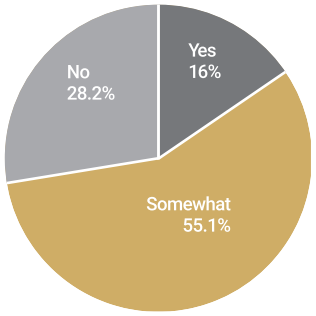
What motivated large entities to purchase cyber insurance in the past 6 months

Risk transfer was overwhelmingly the top choice when brokers were asked what motivated large entities to purchase cyber insurance in the last six months, a consistent trend seen since the survey began in Fall 2015. One respondent also indicated that they thought the current risk/threat landscape was a motivating factor, and another said that large entities purchase cyber insurance for **"broad reputational"** reasons, indicating that boards of directors for larger firms have taken note of the impact on Equifax's reputation following the data breach. Lastly, as with SMEs, **compliance with the EU's GDPR and the NYDFS Cybersecurity Rule** was also said to have influenced larger entities to purchase cyber coverage to some extent.

Policy Language

A clear majority (approximately 83 percent) of respondents said that there was either insufficient clarity from carriers as to what is covered or excluded in a cyber policy, or only somewhat sufficient clarity. Brokers attributed this to "a **lack of commonality** in policy language" and **"too many different forms** all claiming to be the one true version of a cyber policy," and some respondents even went so far as to say that there was a **lack of understanding of what some carriers were insuring due to how rapidly risks evolve.**

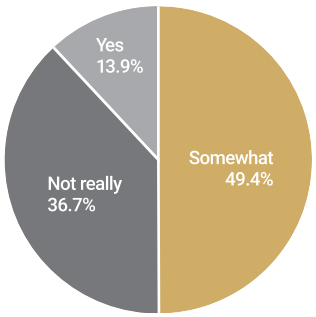
Do you feel there is adequate clarity from carriers as to what is covered and what is excluded in a cyber policy?



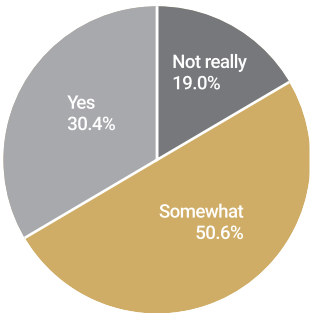
Recent Events

With the advent of the GDPR and the new NYDFS rule, both of which impose fines on companies judged to be noncompliant, organizations may begin to change how they approach and view the purchasing of cyber coverage. As such, respondents were asked whether the recent regulations have changed the way organizations purchase or approach cyber coverage. As seen in the first graph below, **nearly half of respondents (approximately 49 percent)** said that the new regulations hadn't affected their clients' cyber coverage purchasing practices at all.

Have recent regulations affected the way clients approach or purchase cyber coverage? How so?



Have recent cyber events changed the way organizations are purchasing cyber coverage?



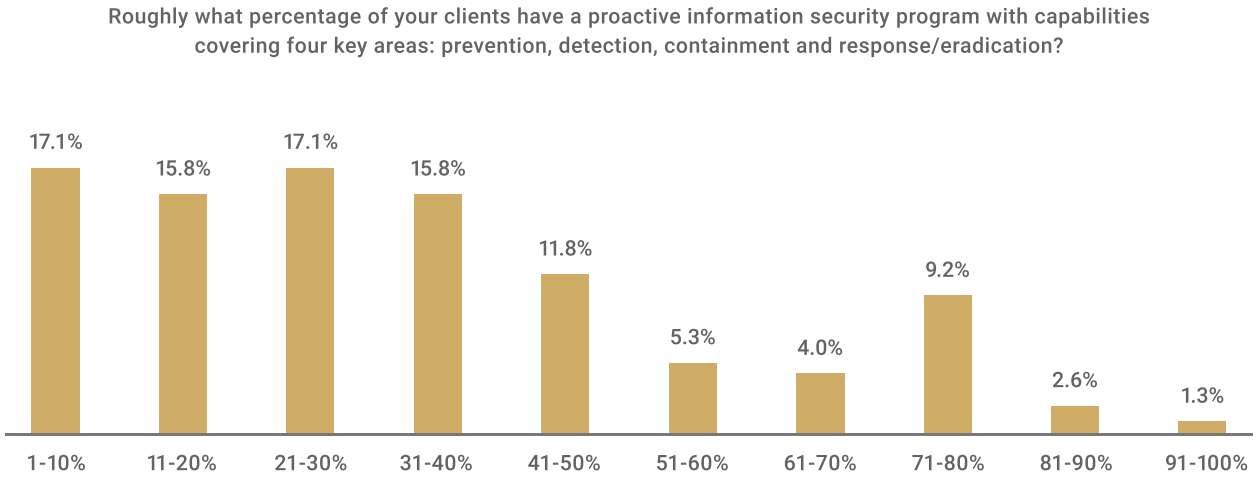
On the other hand, nearly a third (30 percent) of **survey respondents** indicated that recent cyber events, such as the Equifax breach and the WannaCry and Petya ransomware attacks, changed the way organizations purchase cyber coverage, and **slightly more than half (approximately 51 percent)** said that there had been somewhat of a change in their clients' cyber purchasing practices due to the attacks. Additionally, several respondents indicated that both emerging regulations and the treatment of cyberattacks in the news has fueled demand for cyber coverage, with one acknowledging, **"More awareness drove insureds to pull the trigger on purchasing**

cyber." Another respondent from a large national firm said that, thanks to recent events, companies were "starting to realize it was not far-fetched to think they will be a target too."

Education, Marketing & Risk Management

Continuing a trend set in the Fall 2017 survey, **86 percent of respondents reported that they had a proactive, strategic approach to marketing and educating clients and prospects about cyber risks**. Methods utilized by brokers included web-based training (such as webinars or podcasts), examples of cyber claims, seminars, newsletter articles and whitepapers, and making use of pre-renewal/renewal meetings to have a one-on-one discussion of a client's cyber risk and what coverage might be suitable for it. "We treat cyber as a peril and not as a coverage," a respondent from a large national firm said. "We address the exposure across all lines of coverage and offer to engage each of our clients in a strategic analysis of this exposure." Some larger firms also brought on dedicated cyber specialists to deeply explore the intricacies of cyber risk with clients.

Carrier insurance firms also turned to partnering with external cybersecurity organizations to help make their cyber strategy more robust. **Sixty-seven (67) percent of respondents said that carrier insurance firms tend to use these partnerships for both quantifying cyber risk and for post-event response and consulting.** Approximately 27 percent of respondents reported that in their view, these partnerships are used mainly for post-event response and consulting. A respondent from a large national firm noted that in previous years quantifying cyber risk was fee-based, but now brokers are seeing this service offered for free, which may result in more widespread use of partnerships, especially in the lower middle and middle market sectors where, according to a respondent from a midsized Southeastern firm, they are hardly used.



Working with the Federal Government

As in the last survey, respondents were asked their thoughts on what the federal government might do to foster an environment where cyber insurance is widely available, reasonably affordable, and purchased. **Most respondents agreed the government could play a positive role** in helping develop this environment, though approximately 17 percent said that the government should not interfere at all in the cyber insurance market, either because they believed the insurance was already widely available, or because they preferred a more "hands-off" approach regarding government interference in the market.

Of the respondents who believed that the government could do something to help the cyber insurance market, **slightly less than half of them (42 percent)** said that federal standards for data breach reporting and federal

guidelines for safeguarding information systems would be helpful. **About a third of respondents (30 percent)** said that a federal cyber incident information repository would be the most beneficial, which follows a similar trend observed in previous surveys. Moreover, in line with respondents' opinion that there is not yet sufficient clarity in the language that carriers use for policies, several respondents suggested that the government should impose **"consistency/clarity requirements in insurance policies"** as it would make it "easier to read/compare by using same terminology." Others proposed that the government, though not wholly absolving companies from the duty of protecting client data, should **reduce or eliminate fines and penalties** incurred from failing in that duty **if the company has cyber/privacy coverage**. One respondent also simply said that the government ought to "make cyber insurance a requirement," emphasizing brokers' belief that protection is necessary in the face of cyber risks rapidly evolving in both severity and frequency.

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. In 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 seventh Cyber Market Watch Survey will be released in December 2018.

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