# CYBER INSURANCE MARKET WATCH SURVEY
# EXECUTIVE SUMMARY

February 2019

THE COUNCIL

The Council of Insurance Agents & Brokers

## Summary

The Council of Insurance Agents & Brokers (The Council) is pleased to release its seventh biannual Cyber Insurance Market Watch Survey. The survey, which was conducted in December 2018 and consisted of 18 questions designed to provide insights into the burgeoning cyber insurance market, creates a snapshot of the market and allows us to monitor changes and trends.

Survey results showed that **take-up rate remained relatively low** at about **33 percent**, premium pricing stayed **flat to down** and **capacity was flush in the market** (with the exception of specialized industries such as healthcare or drones). Respondents also continued to express a desire for further standardization in cyber policy language, though there were signs that carriers have begun to address this issue. Recent cyber events, such as the Marriott breach, were shown to have affected Council members' and their clients' approach to cyber insurance and cybersecurity. Many respondents also made clear they thought the government could do more when it came to protecting companies and consumers alike from cyber threats.

## Key Findings

### Market Trends

- ✓ 33% of respondents' clients purchased at least some form of cyber coverage
- ✓ 32% of those clients who purchased cyber insurance, 32 percent were first-time buyers
- ✓ 34% of respondents' clients increased their coverage within the past six months
- ✓ 67% of those with cyber insurance have standalone policies

### Pricing Trends

- ✓ $2.8 M was the typical cyber insurance policy limit
- ✓ 87% of respondents said premium prices either stayed the same or decreased over the last six months

### Underwriting

- ✓ 65% of respondents did not see any tightening of carrier underwriting practices in the last six months
- ✓ 23% of respondents believed there was not adequate clarity as to what is included and excluded in a cyber policy
- ✓ 79% of respondents noted that capacity in the market is either plentiful or increasing

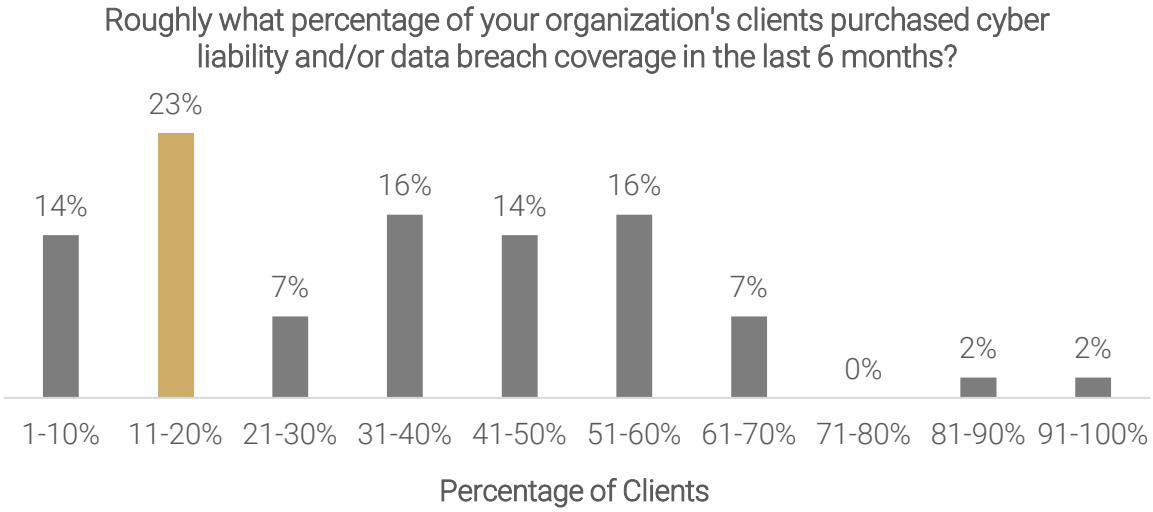
### Cybersecurity/Cyber Risk

- ✓ 85% of respondents' firms have a strategic approach to marketing and educating clients about cyber risks
- ✓ 37% of respondents' clients have an information security program in place focused on prevention, detection, containment and response

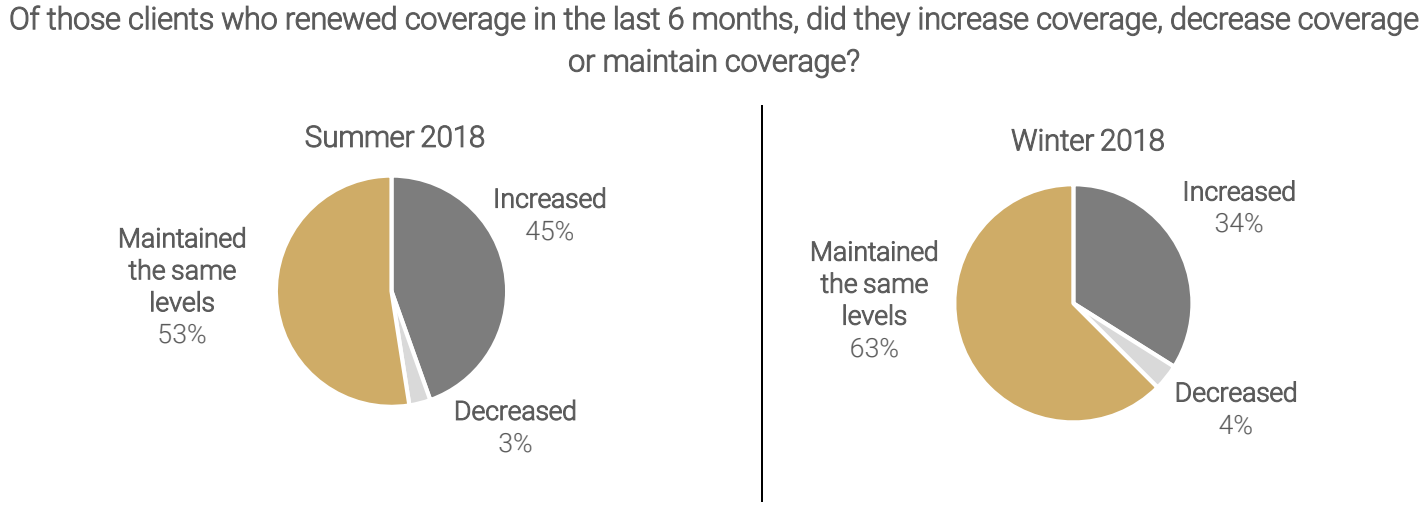
# Survey Highlights

## Take-Up

Take-up rates this quarter remained flat, with about **33 percent of respondents' clients purchasing some form of cyber insurance**, compared to 32 percent of respondents' clients in The Council's Summer 2018 survey and 31 percent in Fall 2017. There were some outliers, however: one respondent from a Southern firm noted that during the past two years they had seen the number of cyber-related policies sold increase dramatically, with more than 50 percent of clients purchasing what their firm offered. Interestingly, another respondent from a midsized Northeastern firm attributed their firm's increase in take-up rate to the fact that carriers were "providing minimum cyber coverage as part of package policy."




The number of first-time buyers of cyber insurance also remained steady: according to respondents, about **32 percent of those who purchased cyber insurance** in the last six months **were purchasing it for the first time**. This did not change from Summer 2018, where 32 percent of those who purchased cyber insurance were first-time buyers. Additionally, **the percentage of respondents' clients who increased their coverage** in the past six months saw an 11 percent drop between this survey and the last, **going from 45 percent to 34 percent.**



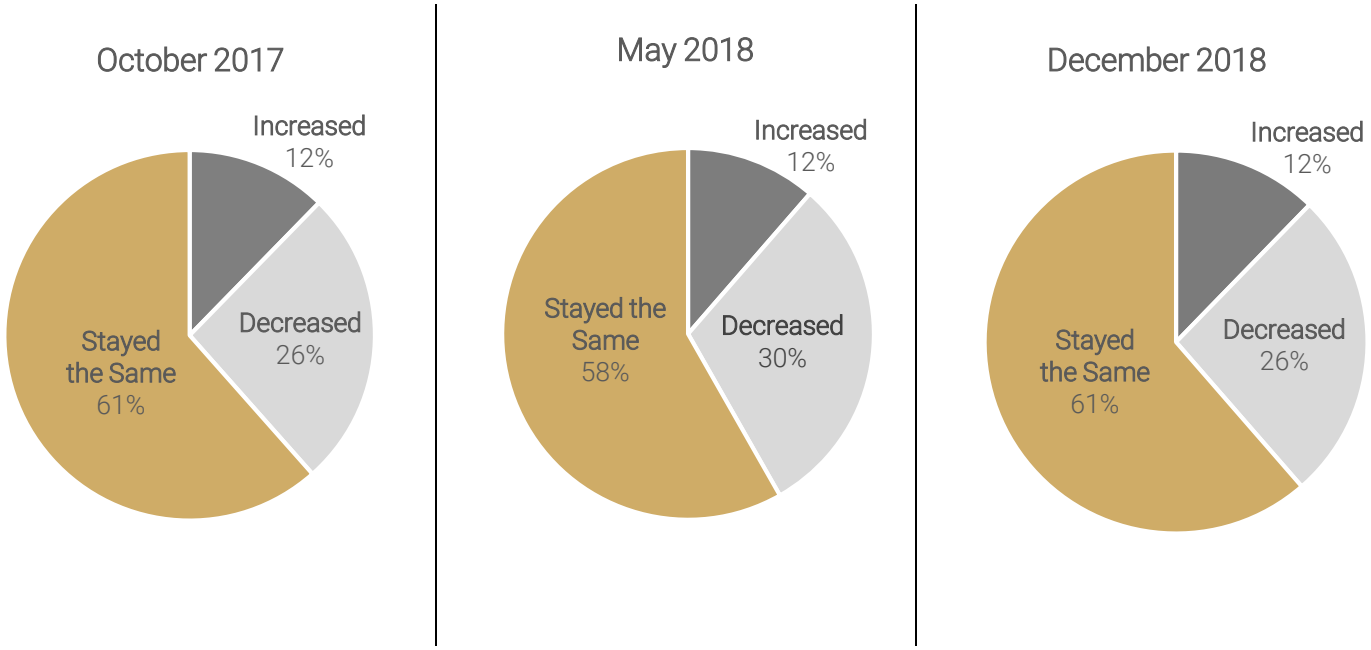
On the other hand, **just 4 percent** of respondents' clients **decreased their coverage** while 63 percent maintained their coverage, showing that most still see cyber coverage as important to have—though "not important enough that the client put more money in their budget for higher limits," as one respondent from a large Southern firm stated.

"While respondents' agreed that clients view cyber insurance as important to have, this did not necessarily translate to clients increasing their budgets for higher limits or increased coverage," explained Ken A. Crerar, President/CEO of The Council. "As a result, take-up rate and coverage levels have remained consistent over the past two years."

## Premium Pricing

Continuing a trend established by previous surveys, premium pricing remained flat-to-down in the past six months. **Sixty-one (61) percent of respondents** said that premium prices for cyber insurance stayed the same and **26 percent** said that premium prices decreased, both very slight changes from the previous survey. As with the Summer 2018 and Fall 2017 surveys, **only 12 percent of respondents** noted an increase in premium pricing. Reasons for the relative stability of premium pricing echoed those given last year: "capacity is flush in the cyber insurance market," said one respondent from a Northeastern firm, though another noted that capacity depended on the industry. Insurance that involved "drones, internet-of-things, etc., was tough to place."

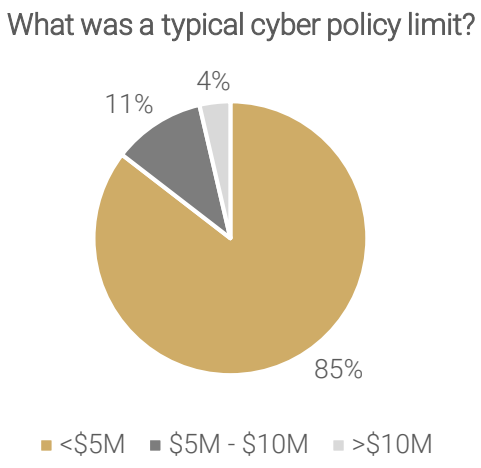
Did premium prices generally increase, decrease or stay the same?

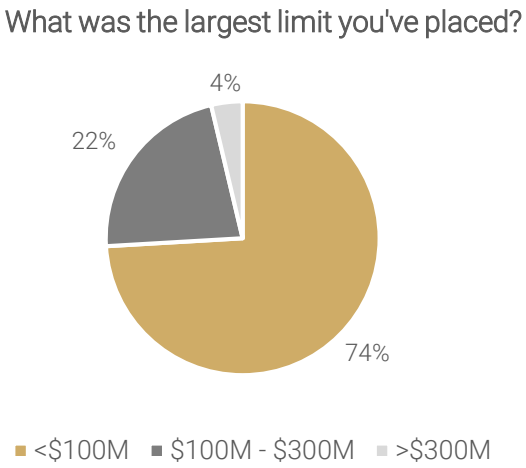



## Limits, Capacity, Product Availability

The average typical policy limit placed **decreased** slightly in the last six months, going from $3.2 million in Summer 2018 to **$2.8 million in Winter 2018**. Apart from several outlier limits ranging from $10 to $25 million, the

vast majority (**85 percent**) of respondents reported typical limits less than or equal to $5 million—very similar to the last survey, where around 80 percent of respondents reported the same.

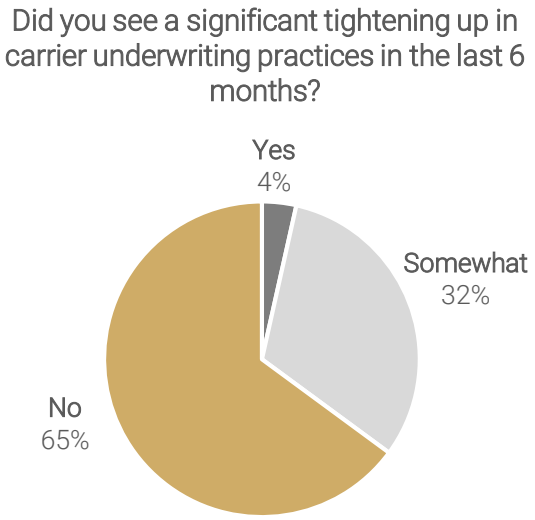



The average **largest** limit placed by brokers within the past six months was approximately **$71 million**. As with other surveys, respondents overwhelmingly (**74 percent**) reported largest limits that fell below $100 million, and around **22 percent** of respondents gave largest limits between $100 million and $300 million. Two firms reported a $500 million tower, a clear outlier, which skewed the calculated average largest limit.

## Underwriting

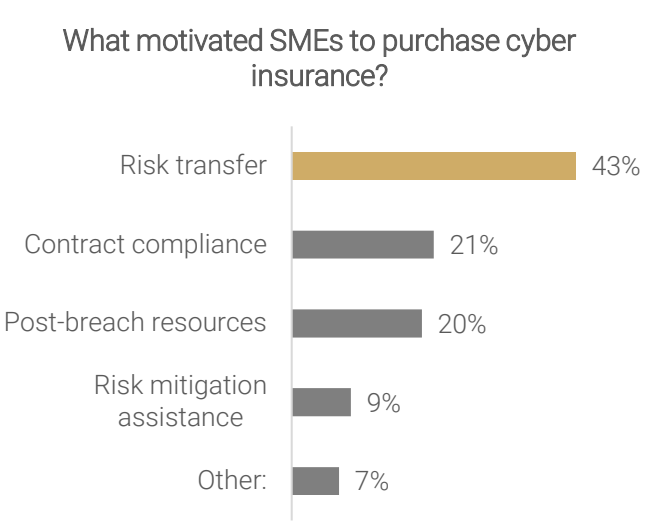
In a slight increase from the Summer 2018 survey, **65 percent** of respondents reported they had not seen **a tightening up in carrier underwriting practices** during the past six months, while **32 percent** of respondents said they had seen somewhat of a tightening up in underwriting practices. Following a trend established by previous surveys, only a fraction of respondents (**4 percent**) said they had seen a definitive increase in carrier underwriting scrutiny.

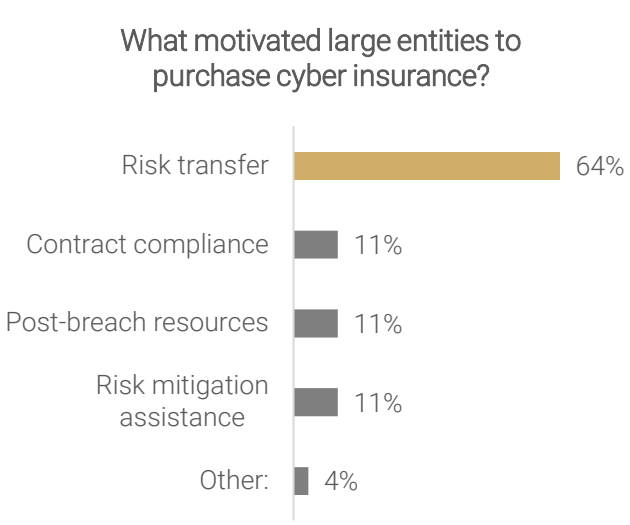



One respondent from a Midwestern firm said the relaxed underwriting practices she had observed were because of **"MANY new markets."** She continued, "The underwriting for virtually all has been relaxed, and we have markets willing to bid for this product." Another respondent from a southwestern firm agreed, stating the carrier **"market was very competitive"** and that it was "easy to get quotes from a few basic questions." However, she added, "for larger accounts it required a completed application in order to get a firm quote." Respondents also agreed that it was noticeably more difficult to get coverage for companies active in the healthcare, cryptocurrency and retail industries—as well as, unsurprisingly, for "clients who aren't taking cybersecurity very seriously."

## Buying Decision

**Risk transfer** was the main factor that drove purchasing of cyber insurance by small- and medium-sized enterprises (SMEs) during the last six months, with **43 percent** of respondents identifying risk transfer as the main reason SMEs made the purchase (an 11 percent increase from the Summer 2018 survey). **Contract compliance** and **post-breach resources** were also relatively important compared to the other factors, with **21 percent** and **20 percent** respectively of respondents naming the two as a motivating factor for the purchase of cyber insurance.



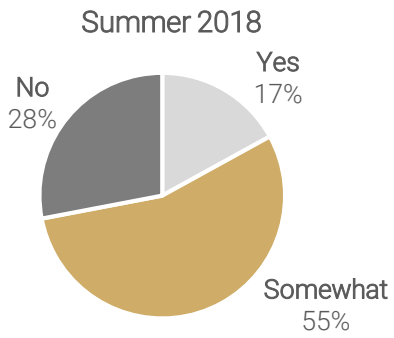



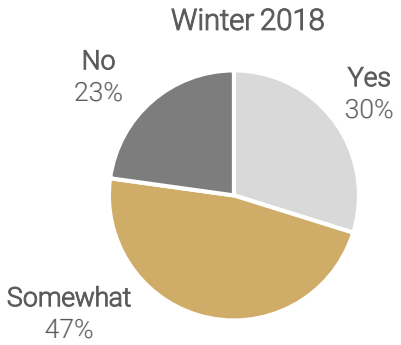

For large entities, **risk transfer** was the clear frontrunner for what motivated respondents' clients to purchase cyber coverage—**64 percent** of respondents selected **risk transfer** as the main driver behind large entities' decision to purchase cyber insurance. One respondent noted that **"education has really helped our clients realize they have a real exposure."** Like most other metrics The Council tracks, this number has hardly shifted over the past few surveys.

## Policy Language

In a first for the Cyber Market Watch survey, approximately **30 percent** of respondents said there was sufficient clarity from carriers as to what was included and excluded in a cyber policy, a number which has nearly doubled from the Summer 2018 (17 percent of respondents) and Fall 2017 (13 percent of respondents) surveys. This may suggest that carriers have been slowly beginning to standardize policy language across the board. Indeed, one respondent from a northeastern firm even said, **"commonality of terms was becoming more prevalent"**, and another from a Southeastern firm mentioned, "many carriers provide marketing sheets describing each coverage."

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



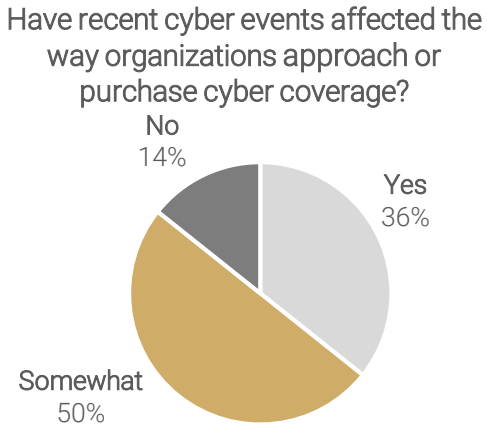



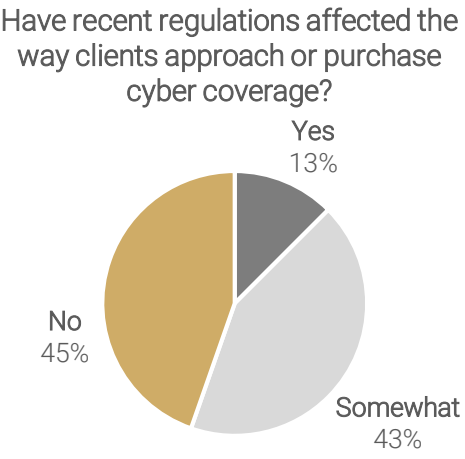

However, it is clear that brokers felt that there are still issues to be resolved regarding cyber policy terminology, considering that **nearly half** (47 percent) of respondents said there was "**somewhat sufficient clarity**" and **nearly a quarter** (23 percent) said there was "**no clarity**" from carriers when it came to what was included or excluded in a cyber policy. One respondent from a southwestern firm said he "would like to see more **standardization** of main coverage grants among all insurers", and another blamed **"semantical differences between carriers"** for confusion between policies.

## Recent Events

Although the WannaCry, Petya and Equifax breaches are old news by now, over the last six months, both the Marriott Starwood database hack (500 million users affected) and the Quora breach (100 million affected) made front page news across the U.S.

There was a solid consensus among respondents that recent events, including these two breaches, have served to change the way their clients think about cyber insurance: **86 percent** of respondents said that recent events either definitely changed or somewhat changed the way their clients purchased or approached cyber insurance, a similar number to the last survey. As one respondent from a northeastern firm put it, **"No one wants to be the company caught flat-footed without cyber".** Another respondent from a Midwestern firm offered a similar assessment: "More of [our clients] recognize the need to buy and budget for cyber" due to the fact cyber events were so widely publicized. **"Even if a client has not had a breach yet,"** wrote one respondent from a Midwestern firm. **"They are starting to know someone who did. They have heard the 'war stories' of what followed."**



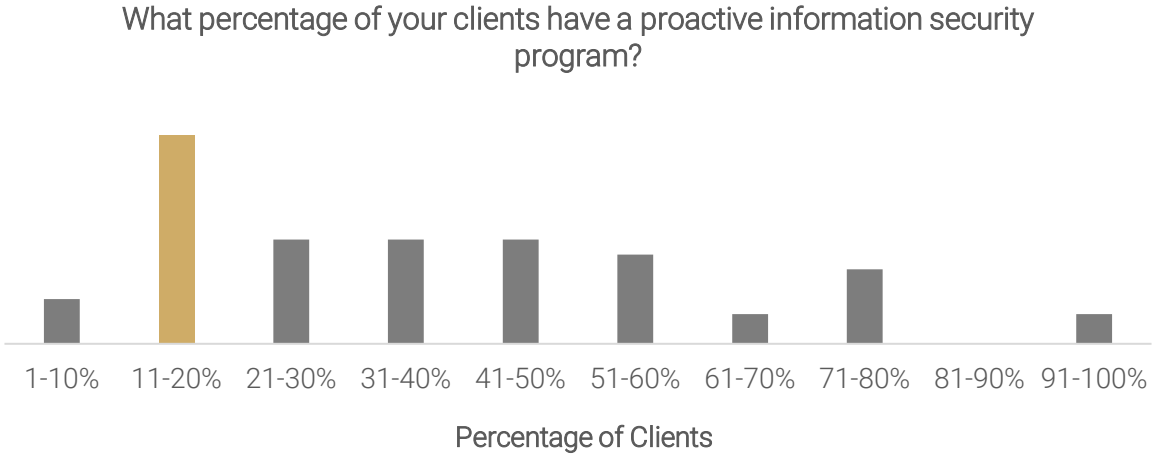



On the regulatory front, cyber policy had less impact on respondents' clients' purchasing practices. A combined **56 percent** of respondents said that recently implemented cyber regulation either **definitely affected** or **somewhat affected** the way their clients approached or purchased cyber insurance, whereas **45 percent** said that recent cyber regulation hadn't affected their clients' approach to cyber insurance at all.

On the whole, respondents agreed that the clients who had been directly affected by regulation like the European Union's General Data Protection Regulation (GDPR) and the New York Department of Financial Services' Cybersecurity Rule were the ones who were starting to ask more questions, such as whether certain fines or penalties would be covered. As more and more states continue to enact or introduce bills and resolutions related to cybersecurity (at least 22 states enacted 52 such bills by November 2018), it will be interesting to see if that might drive more companies to purchase, or at least consider the purchase of, cyber insurance. In September, The Council explored recently-enacted and upcoming cyber legislation: click here for more info.

## Education, Marketing & Risk Management

Brokers continued to make the education of clients one of their main focuses when servicing accounts: **85 percent** of respondents said they had a proactive, strategic approach to marketing cyber insurance as well as to educating their clients about cyber risk. This education varied widely among respondent firms: some brokers tapped into online tools like blogs or webinars, and others used renewal meetings to talk one-on-one with clients about the cyber risks they've faced. Most respondents also mentioned they generally include a recommendation to




purchase cyber insurance on all their proposals.

Despite brokers' efforts, it appears as though their clients have been slower to change when it comes to cyber security. Approximately **37 percent** of respondents' clients have a proactive information security program covering the four key areas of prevention, detection, containment and response/eradication. Respondents agreed that most of their larger accounts are generally more proactive when it comes to implementing data security procedures, which may suggest that lack of resources at smaller companies was a contributing reason for this number.

## Working with the Federal Government

A theme in responses about what the federal government might do to help create an environment in which cyber insurance is widely available, reasonably affordable and purchased was a desire for more proactive regulation. Respondents felt that if regulations obliged companies to go through the steps of loss prevention rather than impose reactive state and federal fines that "are simply insufficient to cause changes in behavior", more businesses would better comprehend the nature of cyber risk and would be more likely to implement effective cybersecurity measures as well as prepare for the inevitable breach by purchasing coverage.

Respondents also continued to push for federal data security and data breach reporting standards, as it would help "simplify the message" and "allow buyers to have a clearer understanding of their obligations". Additionally, some respondents advocated both for imposing a federal framework similar to the California Consumer Privacy Act on every state and for making cyber insurance a requirement for "small, medium and large businesses". In general, it seemed that the majority of respondents agreed that though cyber insurance was already widely available and affordable (one respondent from a northeastern firm estimated that 150 carriers are active in the space and added that "prices are dropping every year"), and the federal government could do more to facilitate purchasing and safeguard consumers themselves from data breaches.

Respondents also highlighted a need for "more communication", which could be done through the creation of a centralized database that would allow them to efficiently share threat indicators.

## 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 eighth Cyber Market Watch Survey will be released in June 2019.

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