CYBER INSURANCE MARKET WATCH SURVEY

EXECUTIVE SUMMARY

October 2016

THE COUNCIL

The Council of Insurance Agents & Brokers

Summary

The Council of Insurance Agents & Brokers (The Council) is pleased to release its third biannual Cyber Insurance Market Watch Survey. Eighty-eight (88) respondents from 66 unique firms participated in the survey, which consisted of 16 questions designed to provide insights into the burgeoning cyber insurance market and create a snapshot of the market to help us monitor changes and trends going forward. This survey would not be possible without our member firms and their willingness to take the time to share their experience and insights into this market. Compared to our April survey, we received 23 more responses from 10 new firms. Respondents observed many positive developments in the market including stabilization of cyber insurance rates, some larger limits being brought to market, and increased take-up rates among clients.

Key Findings

Market Trends

- ✓ **29%** of respondents' clients purchased at least some form of cyber coverage
- ✓ **22%** of respondents' clients purchased cyber insurance for the first time in the past six months
- ✓ **40%** of respondents' clients increased their coverage in the past six months
- ✓ **70%** of those with cyber insurance have standalone policies

Pricing Trends

- ✓ **$3 million** is the typical cyber insurance policy limit
- ✓ **72%** of respondents said premium prices generally stayed the same over the last six months

Underwriting

- ✓ **59%** of respondents have seen some tightening of carrier underwriting practices in the last six months
- ✓ **55%** of respondents believe there is not enough clarity as to what is included and excluded in a cyber policy

Cybersecurity/Cyber Risk

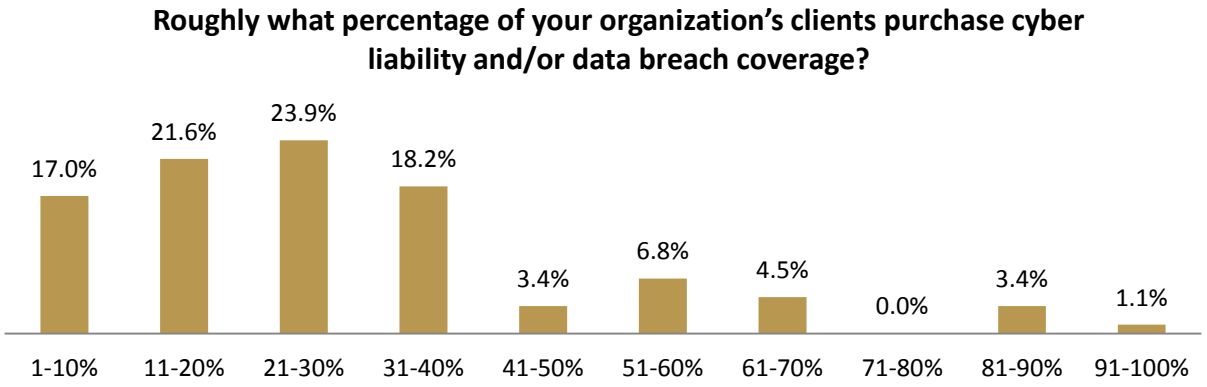
- ✓ **88%** of respondents have a strategic approach to marketing and educating clients about cyber risks
- ✓ **37%** of respondents' clients have an information security in place, focused on covering prevention, detection, containment and response

Survey Highlights

Take-Up

Roughly 29 percent of respondents' clients purchased some form of cyber liability and/or data breach coverage in the last six months, compared to 25 percent in April 2016. This increase follows a slow but steady trend, suggesting that cyber awareness and interest in cyber coverage is on the rise. Respondents' comments also suggest that this number will continue to increase. One respondent said his firm has seen a 15 percent increase in clients purchasing cyber coverage every year for the last three years.

While 29 percent is an average across all sectors and size accounts, 19 percent of brokers responded that 51-100 percent of their clients purchase some form of cyber insurance. Additionally, while some sectors such as Life Sciences and R&D—which do no store much personal or payment information—have historically been less likely to purchase cyber insurance, respondents emphasized their clients in Retail, Healthcare and Financial Services have a much higher take up rate, often around 80 percent.



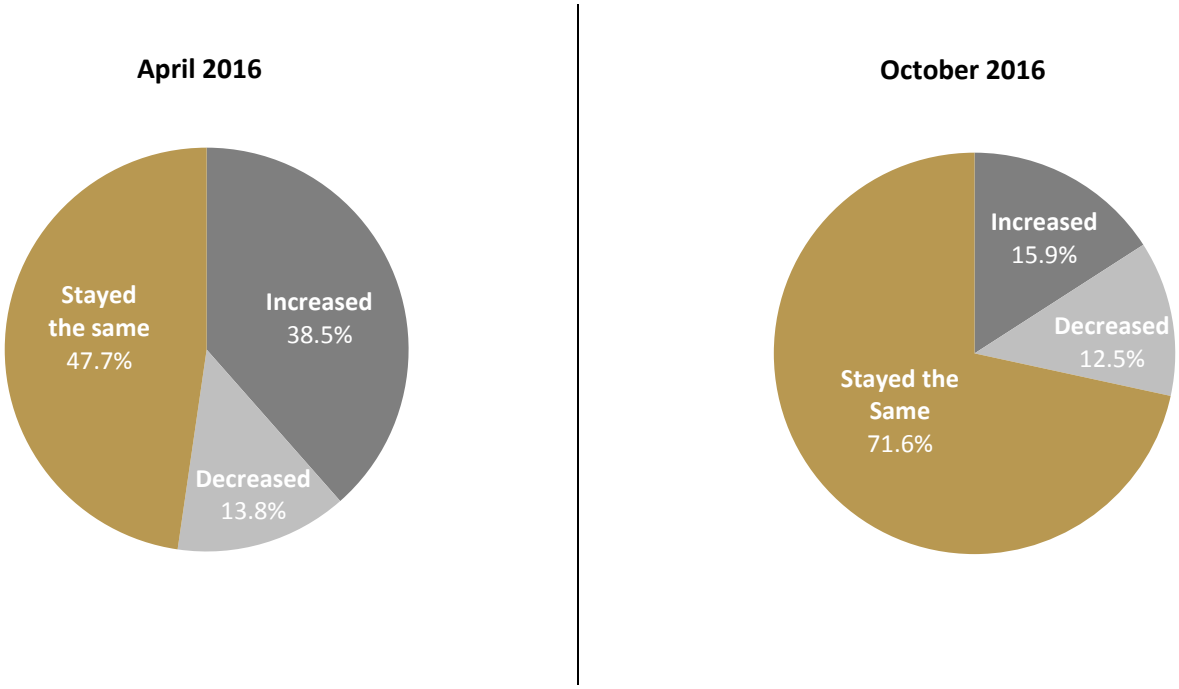
Of those policyholders who purchased cyber coverage in the last six months, **nearly 40 percent increased their coverage levels**. Roughly 60 percent maintained their existing level of coverage and no respondents reported clients decreasing their coverage. While the majority chose to maintain their levels of coverage, we saw **a five percent rise in clients that increased coverage.** This continues to follow the rising trend, proving that more clients are finding value in their cyber insurance policies. One respondent noted that this is "mainly due to increase or improved coverage provided by the market as compared to last renewal," which suggests that carriers are improving and refining their cyber insurance policies.

We also saw an increase in clients choosing standalone policies over embedded. **Seventy (70) percent of respondents' clients choose embedded over standalone,** compared to 66 percent in April 2016. Many respondents emphasized that no one should rely on embedded coverage, as it is quickly disappearing and does not provide acceptable coverage in most cases. One respondent explained, "The coverage available on an embedded basis tends to be very poor. It is frustrating to see so much capacity being devoted to narrow products that provide nearly nothing in terms of risk transfer." This shift toward standalone cyber coverage shows that respondents' clients are beginning to see the real risks associated with data breaches and cyber-attacks, and understand the need for a sound and extensive cybersecurity policy.

Premium Prices

Seventy-two (72) percent of respondents said **premium rates for cyber policies generally stayed the same**, suggesting that underwriting and pricing is beginning to stabilize. In April 2016, only 48 percent of respondents said rates stayed the same and 38 percent said rates increased. One respondent explained that this consistency can be attributed to "increased and or improved coverage provided by the market as compared to last renewal." Another respondent noted that his firm has seen premium prices decrease on small and medium-sized enterprises (SMEs) and increase on their large accounts.

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



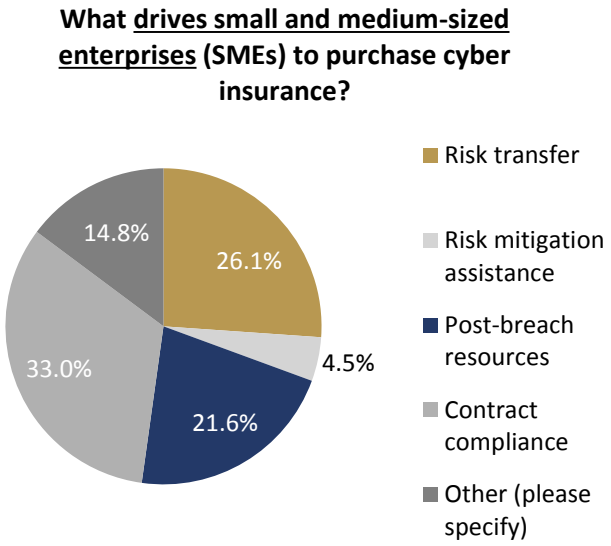
Limits, Capacity, Product Availability

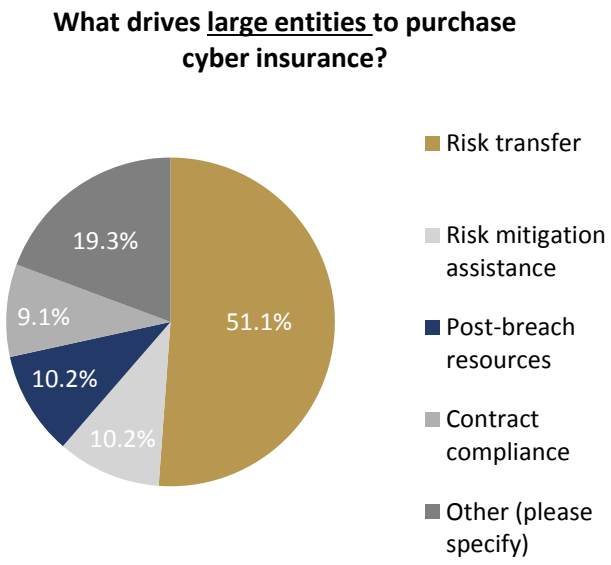
Respondents reported that **the average policy limit is around $3 million**, which is consistent with our April survey findings. This provides further evidence that premium pricing is beginning to solidify – nearly two-thirds of respondents reporting premium pricing staying the same while the average policy limit also remained at $3 million. However, it appears that respondents are placing larger limits for their biggest clients. **The average largest limit was $61 million**, up from $52 million in April. Three respondents have placed policies with limits over $500 million while only one respondent in the April survey reported placing a limit that high.

Respondents had varying experiences with capacity issues in the market. While many respondents noted seeing capacity issues with clients with an extremely high record count, particularly in "tough" sectors such as healthcare, financial and retail, others believe there is still adequate capacity in these areas. One respondent explained that "education has very tight capacity lately [while] large retail is no longer an issue as most insureds have spent more than $50 million in the last couple years on improvements." Healthcare was the sector most often noted as having capacity issues and that sector continues to have the most frequent instances of cyber-attacks.

Buying Decision

When asked the key factor in the decision to purchase cyber insurance, **risk transfer was more of a driver for large entities (51 percent) compared to small and medium-sized entities (26 percent)**. Contract compliance was the leading driver for small and medium-sized entities (33 percent), which plays much less of a role for large entities (nine percent). However, respondents noted that all of these benefits are taken into consideration when deciding to purchase cyber insurance.





Underwriting

In the last six months, **59 percent of respondents saw at least some tightening up in carrier underwriting practices**. Compared to our April survey, where only 43 percent saw some tightening, respondents tended to agree that there has been more scrutiny—especially in the Healthcare, Financial Services, Retail and Education sectors. While carriers have increased their scrutiny of policyholder systems and procedures in certain sectors, one respondent explained, "there are still industries getting very little review in order [for carriers] to gain market share." Another respondent has had experience with some carriers quoting policies based on just a few basic questions or no information at all.

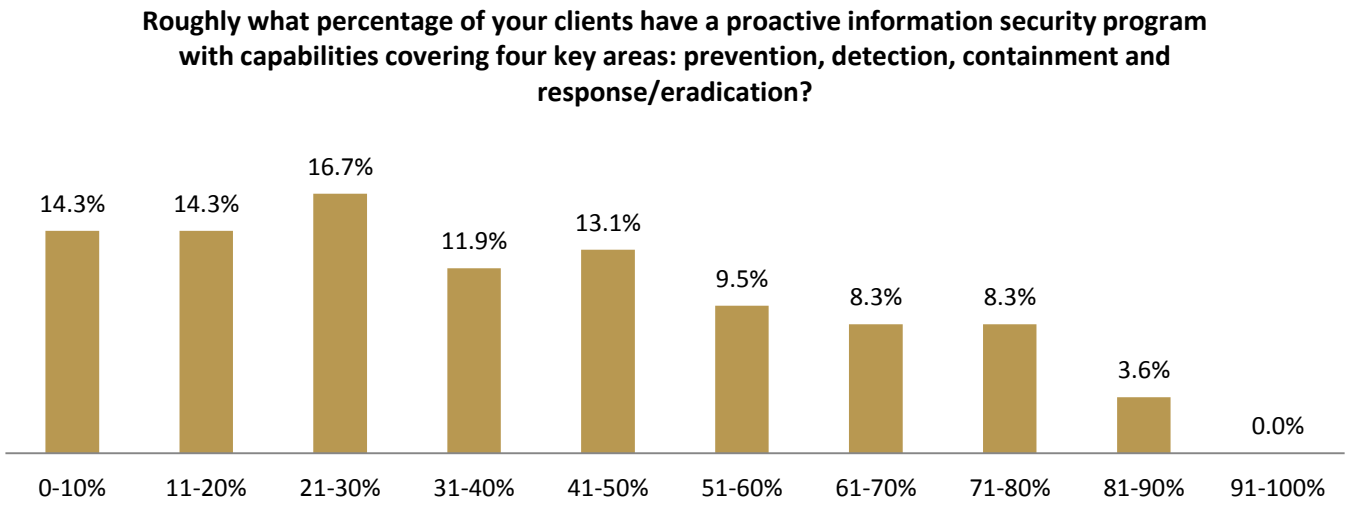
Policy Language

The majority of respondents (55 percent) feel there is not enough clarity from carriers as to what is covered and what is excluded in their cyber policies. Many respondents noted that coverage is still being written via manuscript policies, leading to different terminology from carrier to carrier. To combat this issue, one respondent explained "there needs to be standardization so that we know what we're selling and the client understands what they are buying. Is it Cyber, Data Breach, Privacy & Security, etc.?" It is important to note that several respondents do believe there is adequate clarity, or as much as there can be, but the responsibility falls on the broker to understand and explain this language to the client. While it is evident progress is being made on this front, especially in the wholesale marketplace, many brokers feel that a common lexicon would be tremendous in helping clarify cyber policy language.

Education, Marketing & Risk Management

Brokers continue to be integral in educating their clients about cyber risk and their individual exposures. Eighty-eight (88) 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 include webinars, seminars, whitepapers, client meetings upon renewal, email publications, blogs and mailings.

However, much still needs to be done and implementation of risk mitigation measures is still inadequate. Only 37 percent of respondents' clients have a proactive information security program in place with capabilities in four key areas: prevention, detection, containment and response/eradication. This number aligns with our April findings (35 percent), suggesting that progress is slow as entities struggle to stretch tight budgets to adopt cyber defenses. Without sufficient front-end cyber protection, organizations put themselves at a significant risk of cybercrime and even breaches that are not malicious. Therefore, it is crucial that companies understand that much of what is lost cannot be recovered following a cyber-attack or data breach - intellectual property, transferred funds, unhappy customers, reputational damage, etc. – even if cyber insurance is in place and covers an event.



Strategic Partnerships

Partnerships between carriers and cybersecurity firms, and even brokers and cybersecurity firms, have been prevalent in the market. **The majority (60 percent) of respondents believe that these partnerships are beneficial for post-event response and consulting, but not for pre-event risk quantification.** Many brokers believe that the carriers have yet to utilize these partnerships in the most effective way. One respondent explained, "right now they need to fine tune the offering to make these partnerships more strategic and valuable to clients." While we have been seeing an uptick in these partnerships lately, they are still in the early stages and will improve over time. They will also become more valuable as a risk quantification tool as the industry collects more actuarial data on cyber risk.

Working with the Federal Government

Respondents believe that there are measures the federal government could implement to help support the availability and evolution of cyber coverage. These measures include: tax credits on premiums; a federal standard for data breach reporting; a cyber incident data repository; and federal guidelines for safeguarding information systems. Many of these measures are already being implemented or in the discussion phase. Members of Congress have been vocal about their desire to be helpful in the cyber space, as well, and several bills and initiatives have been introduced in recent months.

Cyber Incident Data Analysis Repository (CIDAR)

The Department of Homeland Security (DHS) created the Cyber Incident Data and Analysis Working Group (CIDAWG) to design a repository of cyber incident data. The group is currently finalizing what input fields would be included and exploring a pilot program.

Cyber Information Sharing Act (CISA)

CISA was passed by Congress and signed into law by President Obama in December 2015. This program was designed to provide liability protections for entities that share cyber threat information with the federal government and among other private sector entities. In accordance with CISA, DHS created the free Automated Indication Sharing (AIS) program, which enables the sharing of cyber threat indicators between the private sector and federal government in real time. While entities have been slow to sign on, DHS is encouraging more organizations to participate in the program.

Presidential Policy Directive 41 (PPD-41)

President Obama created PPD-41 as part of his Cybersecurity National Action Plan (CNAP) executive order. PPD-41 aimed to help the federal government coordinate with the private sector when responding to cyber-attacks. In September, DHS released a draft national cyber-incident response plan, seeking comments from the private sector to further Presidential directive, which will be finalized by 2017.

The Data Breach Insurance Act (H.R. 6032)

Congressman Ed Perlmutter (D-CO) introduced the first piece of legislation pertaining specifically to cyber insurance. The Data Breach Insurance Act (H.R. 6032) would provide a tax credit equal to 15 percent of cyber insurance premiums to organizations that purchase coverage and adopt the NIST Cybersecurity Framework. This "two-prong approach" will ideally increase companies' cybersecurity defenses on the front-end, as well as help them recover from a cyber incident.

The Improving Small Business Cybersecurity Act (H.R. 5064)

The House passed a bill in September that would allow Small-Business Development Centers (SMBCs) to assist small business on cybersecurity matters. The Improving Small Business Cyber Security Act (H.R. 5064) would help solve the cyber "expertise gap" that small businesses face and would address the assertion that cybersecurity laws pertain to and unfairly assist larger businesses.

Conclusion

The last six months were once again full of cyber activity and developments. Yahoo recently discovered that hackers stole more than 500 million user accounts in 2014; ransomware has increased by nearly 500 percent; and state-sponsored actors have been relentlessly hacking into government networks and releasing information to the public. While these events and the rise of cybercrime certainly raise cyber awareness and spark interest in cyber insurance, there is still progress to be made.

Fortunately, brokers saw improvements in nearly all the aspects of cybersecurity and cyber insurance. Cyber insurance take-up rates are on the rise, with slow but consistent growth. Organizations, for the most part, seem to be increasing their coverage levels and brokers suggest that there is still adequate capacity across most sectors. Additionally, premium pricing has largely stayed steady over the last year which suggests that the market is stabilizing. Companies choose to purchase cyber insurance for a variety of reasons, including risk transfer, risk mitigation, post breach resources and contract compliance. And lastly, while companies need to be make it an operational imperative to define and manage cyber risk as an enterprise risk issue, brokers are playing a key role in educating their clients and prospects about actions and considerations that will drive the organization to become more resilient. Cyber risk is unique in that you not dealing with a natural science but rather a social science and human behavior. It is going to get worse before it gets better and it's getting companies to do the 20 percent that gets them to the 80 percent. It is a fool's errand to try and protect everything. Nonetheless, the cyber insurance market has a tremendous opportunity to play a key role in helping organizations both prevent and respond to cybercrime.

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 fourth Cyber Market Watch survey will be released in April 2017. For more information on the survey, please contact Rob Boyce, The Council's Industry Affairs Associate, at Robert.Boyce@ciab.com.