CYBER INSURANCE MARKET WATCH SURVEY EXECUTIVE SUMMARY

April 2016

THE COUNCIL

The Council of Insurance Agents & Brokers

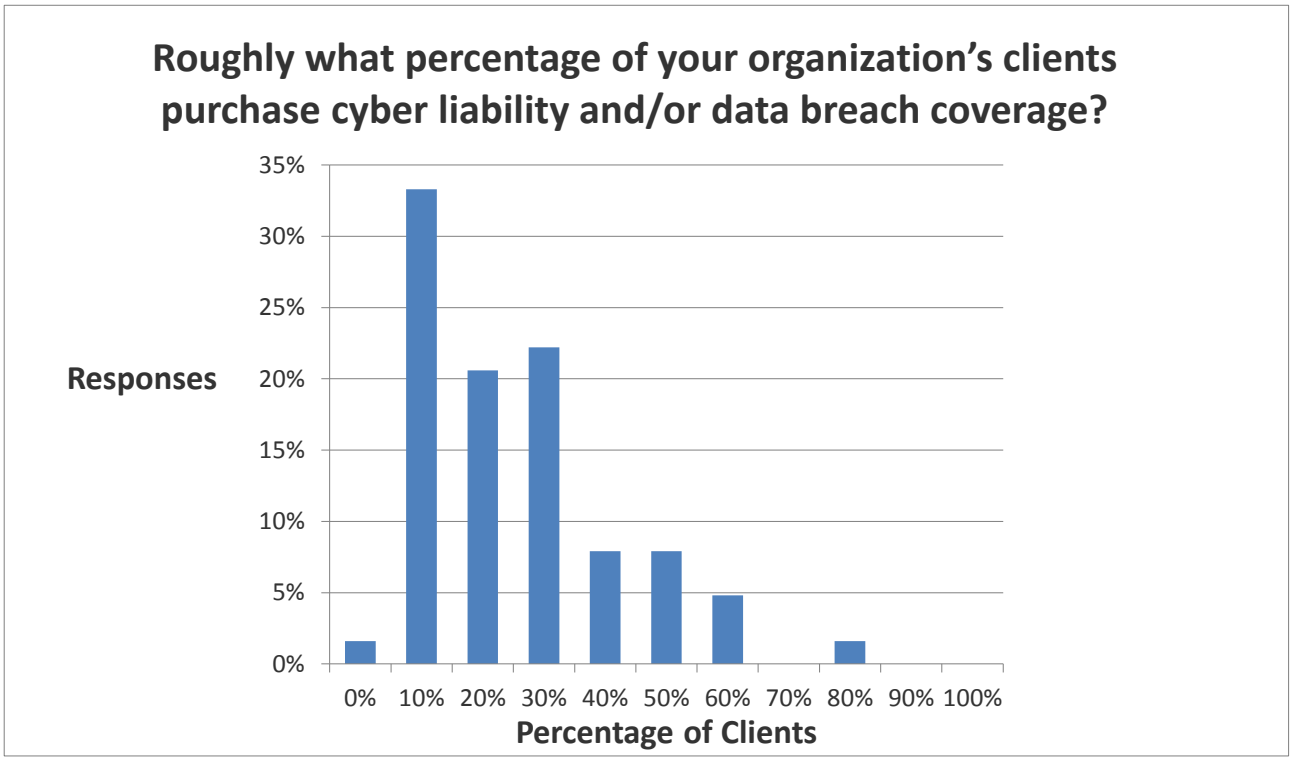
Summary

The Council of Insurance Agents and Brokers (The Council) is pleased to release the results of its second semi-annual Cyber Insurance Market Watch Survey. Sixty-five (65) respondents from 56 unique member firms responded to a set of 18 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. We expanded this second round of the survey by adding seven questions designed to help us dive deeper into the broker's experience with the underwriter and with the client when selling a cyber policy. We also asked participants to expand upon some existing questions in order to glean greater insights into how brokers are educating their clients and marketing cyber products and how clients are making their buying decisions.

Survey Highlights

Take-Up

Approximately 25 percent of respondents' clients purchase some form of cyber liability and/or data breach coverage. This is consistent with responses from the fall 2015 survey, but with a slight uptick in higher percentages. In October 2015, the highest percentage of any brokers' clients that had purchased coverage was 60 percent, but this time there were a handful of respondents who had upwards of 80 percent of their clients purchase this coverage. This demonstrates that while growth in take-up rates was small, there has been gradual growth.



Of those policyholders that purchased cyber coverage in the last six months, approximately 32 percent purchased it for the first time. Of those clients that renewed their cyber coverage in the last six months, roughly 65 percent maintained their existing level of coverage, while 35 percent increased coverage. No respondents reported decreases in coverage. This is consistent with results

reported in October 2015 and suggests that clients find value in their cyber insurance coverage. Several respondents commented that certain high-target sectors, such as health care, were more likely to increase their limits when possible.

Survey responses also showed a slight increase in clients electing standalone cyber policies over embedded coverage in traditional lines. Respondents reported that approximately 66 percent of their clients purchase standalone policies, versus 34 percent relying on embedded coverage. One respondent from a regional broker in Ohio remarked, "We are attempting to dissuade embedded or endorsed partial coverages, including perceived coverage in Professional Liability policies and pushing the standalone coverage." A respondent from a national broker on the west coast added, "Most clients understand that embedded coverage is very limited."

Buying Decision

The key factor in the decision to purchase cyber insurance, across all size firms, is the desire to transfer risk. Small and medium-sized enterprises (SMEs) are compelled to purchase cyber insurance mainly to transfer risk (38 percent) and for the post-breach resources many carriers and brokers provide (25 percent). Large entities are similarly motivated by risk transfer (51 percent) and post-breach response resources (25 percent). Interestingly, large entities are more interested in the risk mitigation services offered by carriers and brokers (15 percent) than smaller entities (5 percent) and small and medium-sized entities are more motivated by the need to fulfill contractual requirements to maintain cyber insurance (23 percent) than larger entities (6 percent).

Premium Prices

Survey responses indicate that premium rates were generally stable in the current environment over the past six months. Forty-eight (48) percent of respondents said that rates essentially stayed the same, while 38 percent said rates increased, and 14 percent indicated rates decreased. These responses show a slight increase in rates compared to the previous six months. In October 2015, 55 percent of respondents said that prices had stayed the same, while only 28 percent said rates had increased. Respondents stressed that rates (along with availability and limits) vary widely by industry and firm size. According to one large international broker, rates vary "dramatically by industry and size. But the major price increases seem to have been taken in 2015." Another national broker based in Georgia commented that rates "decreased for smaller, simpler risks due to strong market competition."

Underwriting

When asked whether they experienced a significant tightening in carriers' underwriting practices in the first quarter of 2016, participants were split. Thirty-one (31) percent said that there was probably some tightening, while 43 percent said it was not likely. Twelve (12) percent indicated that there has "definitely" been a tightening in underwriting standards. Underwriting practices vary widely from carrier to carrier and also by industry and firm size. Some carriers have simplified forms and will provide a quote based on just a few questions. Others are asking more questions and increasing scrutiny, particularly for high-risk targets such as cloud vendors, payment processing vendors, health care, technology and finance.

The jury is still out on whether or not the partnerships insurance companies are forming with firms—modeling, cybersecurity and/or technology—are sufficient to help them quantify cyber risk. Fifty-five (55) percent of respondents were unsure, while approximately 34 percent felt that these partnerships are insufficient to quantify cyber risk. The lack of actuarial and cyber incident data is a topic being examined at length by both the insurance industry and state and federal lawmakers and regulators. The nature of cyber risk is man-made and constantly changing in order to overcome cyber defenses. Modeling firms are starting to create models but no model is ever perfect. A solution, other than experience and data acquired over time, has yet to be proposed. As one bank-

owned regional broker observed, current risk quantification is “not fully sufficient, but a step in the right direction.”

Policy Language

Cyber coverage continues to be written via manuscript policies with vastly different definitions, terminology, limits, endorsements and exclusions. Brokers must be careful to read policies thoroughly in order to know exactly what is included and what is excluded and provide educated advice to their clients. As one large national broker noted, “There are no standardized forms, so you need to scrutinize each placement carefully.” Because of this variability in forms from carrier to carrier, some brokers are choosing to work with a select few. That same broker explained, “This is why we tend to work with relatively few carriers. It is too difficult to compare offerings, coverage enhancements and exclusions with too many carriers. It can be overwhelming.”

Limits, Capacity, Product Availability

Respondents reported that the average policy limit is typically around $3 million. This is up from $2.4 million reported in the previous six months. The average largest limit respondents have placed is approximately $52 million, up slightly from $50.7 million reported in the previous six months. The largest tower assembled is still $500 million.

Respondents indicated they are finding adequate capacity in the market for their clients’ needs and desired coverage, especially for lower limits and the least risky clients. One broker in the northeast focused on serving the business insurance needs of middle market companies explained that there is “more capacity emerging at the low end of the market; in classes least exposed – classic toe-dipping by the newer players. Capacity constriction is taking place in working program layers in higher exposure industry segments.” Respondents did note some capacity restrictions in high-target industries such as finance, health care and retail.

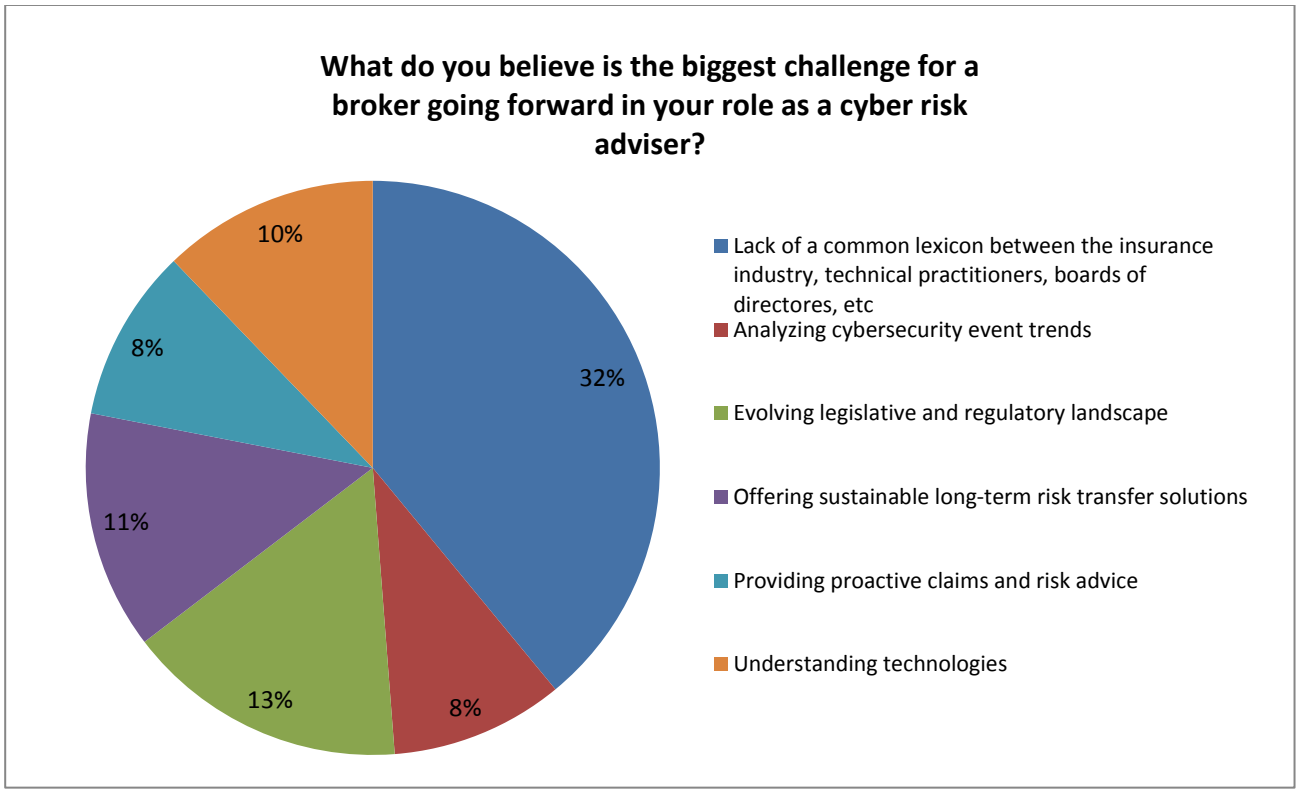
We asked survey participants to tell us what needs to happen in order to increase the types of cyber insurance products—such as coverage for loss of intellectual property, physical damage, bodily injury and contingent business interruption—available to policyholders. Respondents agreed that these products will develop over time. The industry needs a longer claims history and more event data. Events that are not covered by existing policies will expose gaps in coverage. One bank-owned broker concentrated in the South suggested that “Limited case law and untested coverage forms create confusion with carrier products as well as client commitment to purchase the coverage.” Insurers and policyholders will test policy language in coverage disputes and there are already cases that have been decided or are pending in court. Another bank-owned broker based in the South expounded, “The market will naturally broaden where carriers see opportunities and where they feel they can appropriately assess the risk. Look to how the market slowly began to offer things like Business Income and Cyber Crime which continue to move toward being a consistent grant.”

Education & Marketing, Risk Management and the Role of the Broker

Eighty-seven (87) percent of respondents’ firms have some proactive, strategic approach to marketing and educating clients and prospects about cyber risk. Strategies vary from simply pitching cyber products at every renewal, to more regular educational offerings such as newsletters, in-person client training, programs by outside vendors, seminars and dedicated internal cyber teams.

Much more must be done to educate clients about their cyber risks. Only 35 percent of respondents’ clients have an information security program in place with capabilities covering prevention, detection, containment and response/eradication. This leaves these companies extremely vulnerable to cyber-attack, non-malicious data breach and irreparable financial and reputational damage to their businesses.

Most brokers, 38 percent of respondents, believe their long-term role in managing cyber risk for their clients is to be a proactive adviser on trends and developments in this new breed of risk. Many others, 26 percent, believe the primary role of the broker is to facilitate risk transfer and risk financing by placing those products for their clients. Seventeen (17) percent of respondents believe the role of the broker is to drive sustainable, long-term strategic advisory and risk management services. Other roles suggested by respondents included educator, strategic advisor, and claims, compliance and forensic support. Overwhelmingly, 51 percent of respondents believe the biggest challenge for brokers as cyber risk advisors is the lack of a common lexicon among the insurance industry, technical practitioners, boards of directors, regulators and other stakeholders. Other challenges include the evolving legislative and regulatory landscape and offering sustainable, long-term risk transfer solutions.



Conclusion

The cyber insurance market continues to develop at a slow, but steady pace. During the fourth quarter 2015 and first quarter 2016, rates were stable to slightly rising and take-up increased across all industries. Capacity has been plentiful at lower limits and for the least risky profiles. Brokers continue to be challenged finding adequate limits for the high-target industries (finance, health care, education, technology) and larger firms, especially those that maintain Personally Identifiable Information (PII), Personal Health Information (PHI), and Payment Card Information (PCI). Brokers play an important role, not just as the mechanism for risk transfer, but in helping clients understand their cyber risks and what is included and excluded in a cyber insurance policy. By taking a more holistic view of the role of the broker in cyber insurance—as educator, policy expert, translator, risk manager and first responder – the broker can provide exceptional value to their clients.

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 in-depth findings are exclusive to survey participants. The Council's Cyber Insurance Market Watch is released on a biannual basis. The next survey will be released in October 2016. For more information on the survey, please contact Amy Roberti, The Council's vice president of industry affairs, at amy.roberti@ciab.com.