MARSHBERRY

channelcheck

Is There A **Communication Breakdown?**

MarshBerry Cyber Insurance Channel Check

07 | 18

Introduction

Reports are that the market for cyber insurance is growing. A.M. Best reported that "The U.S. market for cyber insurance grew significantly in 2017, as direct premiums written rose nearly 32 percent year over year to $1.8 billion, and policies in force jumped 24 percent to $2.6 million". Although this rate of increase is off of a relatively small base in the prior year, it reflects that people are starting to get the message about the risks of cyber-crime.

But is everyone getting the message about the dangers of cyber-crime? The answer appears to be "no". Current cyber insurance demand is being driven by large commercial entities (national accounts and Fortune 500 companies). Meanwhile the take-up rate for small to medium size companies is in the low teens (compared to the 32% overall increase). While at MarshBerry we see cyber as a growing market and area of opportunity we wanted to gather insights about drivers of demand and how Agents/Brokers can sell this coverage.

QUESTIONS WE ARE ADDRESSING INCLUDE:

1. ***How are agencies/brokers selling cyber?***
2. ***Who is buying cyber, and why?***
3. ***How can one convince clients of cyber-related risks and why they need coverage?***

We are pleased to present the results of primary research held with distributors and users of cyber insurance in the United States. We also included a primer on cyber.

Key Takeaways

DEMAND

- Demand for cyber insurance was reported by channel check respondents as approximately 7.5% higher on a year-over-year basis. However, some respondents see a major drop off in the up-take from initial inquiry to actual purchase.
- Demand was reported to be mostly driven by: 1) increased awareness of cyber risks amongst smaller revenue commercial and educational entities, and 2) B2B relationship contract requirements.
- In MarshBerry's experience, education regarding cyber risks across the insurance distribution channel including Insurer, Agent/Broker and Insured is essential.

PRICING

- Overall average cyber insurance premiums remain relatively tepid and flat year-over-year, restrained by insurer competition along with up-take rates.
- Many respondents commented that they expect cyber-crime (and publicity on breaches) will continue to be high and that they feel uncertain about adequate pricing of risks in current policies once claims materialize.

UNDERWRITING CAPACITY AND ADEQUACY OF COVERAGE

- Underwriting capacity was reported as mixed with some respondents commenting that questions/applications for cyber insurance are improved with more pertinent and targeted questions due to recent insurer experience with cyber related claims.
- Reported concerns remain about adequacy of coverage and complete understanding related to what is or is not covered in many policies.

Demand

In the first half of 2018, demand for cyber insurance was reported by cyber channel check respondents as approximately 7.5% higher on average on a year-over-year basis. However, there is relative variability in the level of reported increase, which is different than in our past Channel Checks on cyber insurance. While all respondents to our study reported that they automatically include cyber insurance in their proposals to clients, the up-take from initial inquiry to actual purchase sees a major drop off for some respondents. For example, the percentage increase in inquiries is reportedly 15% higher than last year, but actual purchase of cyber-insurance is a fraction higher (approximately 2.5%). Interestingly, the outlook for 2018/2019 demand is "increased" amongst all respondents.

Per our respondents, cyber insurance demand is mostly driven by: 1) increased awareness of cyber risks amongst commercial clients, especially smaller revenue commercial and educational entities, and 2) B2B relationships. Many B2B contracts are stipulating cyber (first party and/or third party) coverage to establish and/or continue a supplier relationship.

Diversity of commercial clients has increased. In the past, traditional industries dominating the cyber insurance space have been health care and retail – this is changing. The diversity of industries taking up cyber insurance has increased with educational institutions and smaller commercial clients reflecting the greatest uptick in reported recent demand.

In MarshBerry's experience, and in this study, education across the insurance distribution channel from Insurer to Agent/Broker to Insured is essential. First, we anticipate that a greater understanding of cyber risks and impacted technologies would assist insurance Agents/Brokers to explain pertinent cyber risks and coverage options to clients. Second, once commercial and personal clients have a greater understanding of the possible threats and loss in recovery (including but not limited to cyber extortion and ransomware, risk of shutting down the company, identity theft, expense of post-breach services, legal and extreme reputational risk) from cyber-crime, they are more willing to engage. A more effective communication of potential cyber risks would lead to a higher take up rate (especially at relatively low current pricing).

- A Broker from the South reports: *"Demand is 5% higher year-over-year because companies want to make sure they can sleep at night. By industry the uptick is in healthcare (still #1) and education is #2. A lot of school districts and colleges want cyber now."*
- A Senior Executive from a Western-based Agency/Broker stated: *"Smaller companies are more open to buying cyber because more acceptable and less expensive options are more readily available."*
- A Senior Executive from a Northeast Agency/Broker had a very different view and commented that: *"It appears that there is hard traffic in learning tools and quotes - but then the number of clicks on actually buying cyber insurance sees a massive drop off. The approximate 15% interested in researching cyber insurance drops to under 0.5% buying cyber insurance."*
- An Executive in a Southeast-based Agency/Broker reported: *"Smaller companies in the $10MM to $50MM revenue range have seen the biggest increase in cyber insurance demand. The larger companies typically want to self-insure."*
- An Executive in a Northeast-based Agency/Broker reported: *"A major issue around demand for cyber coverage is education of insurance Agency/Brokers and their need to get more comfortable discussing cyber risks with clients."*

Pricing

Overall average premiums remain relatively tepid and flat on a year-over-year basis in our respondents' experience in the first half of 2018. The market is described as "soft" (the same as in previous Cyber Channel Checks) by most respondents. However, for some the "soft" versus "hard" market depends on the type of client and their perceived exposure. Limits were reported as unchanged on a year-over-year basis. Looking forward into the next one to three years, the premium outlook is for higher pricing amongst all our respondents. Respondents commented on their expectation that cyber-crime (and publicity on breaches) will continue to be high and their uncertainty about adequate pricing of risks in current policies once claims materialize.

- An Executive in a Southeast-based Agency/Broker reported: *"Our outlook is higher crime/claims frequency, so we see pricing going up. Right now, pricing is low, and we are scratching our head on how underwriters are offering these pricing policies."*
- An Executive in the Northeast commented that: *"Pricing is NOT soft for high exposure records, excess limits, and excess*

At MarshBerry, we see cyber insurance as a **growing market and area of opportunity.**

$5 million+ primary coverage. Although pricing is softening, it is not the same for anyone who has a large number of entry points, develop own software, needs excess limits, media and had large data - for these people/organizations, pricing is hard."

- A Southern-based Agency/Broker owner stated that: *"We have seen a proliferation of $3K to $5K premium range. There is more acceptability when there are only five questions to answer."*

Underwriting Capacity and Adequacy Coverage

Relatively high Carrier capacity to underwrite cyber insurance was described by all respondents (which is the same as in our prior Cyber Channel Checks). Questions and applications for cyber insurance were reported as improved with more pertinent and targeted questions due to recent insurer experience with cyber related claims. In addition, the reported shortened list of questions that were more applicable to smaller commercial clients were appreciated by our respondents. However, other respondents reported an absence of understanding behind the underwriting.

Reported concerns remain about adequacy of coverage and complete understanding related to what is or is not covered in many policies. For example, one respondent reported that during a recent cyber attack at a commercial client the insurer "did not have proper risk management processes and were not prepared properly to manage forensics work quickly. With cyber, if attacked it is like a fire, but our insurance company partners are taking a couple of days to respond in our experience, which is far too long."

- A Northern-based Senior Executive said that: *"The granularity of questions increases substantially with the size of the limit."*
- A Midwest-based Agency/Broker owner stated: *"The market has recognized that insurers need to improve the ease of use and make underwriting match risks more closely. They used to have seven pages of discussion for a small sole proprietorship and now the questions are shortened to fit the risk."*
- A Western-region entrepreneur commented that: *"It is clear that the underwriting questions asked are more comprehensive on applications due to more experience on the part of insurance companies who have also experienced losses."*
- A Midwest-region Agency/Broker commented that: *"Underwriting had more loss activity and some big ones in the last year alone. We have experience with twelve claims and two being large related to bitcoin. These companies were shut down and forensics work alone cost $80K to $100K."*

AUTHORED BY

Alison Wolf,
Director – Research
440.637.8119
Alison.Wolf@MarshBerry.com

Engage Online

28601 Chagrin Blvd., Ste. 400
Woodmere, OH 44122

www.MarshBerry.com

@marshberryinc

facebook.com/MarshBerry

linkedin.com/company/MarshBerry

MarshBerry.com/blog

Need help identifying where your agency should focus?

Call MarshBerry for a strategy consultation at **800.426.2774** or visit us online at **www.MarshBerry.com.**

Cyber Risks Primer

'CYBER RISK'

The risk an organization takes on from failure of their IT systems making it susceptible to anything from financial losses to disruptions or damages to the organization itself.
https://www.theirm.org/knowledge-and-resources/thought-leadership/cyber-risk/

CYBERCRIME

Any criminal activity that involves a computer, networked device or a network. The two primary categories of cybercrime include advanced cybercrime, composed of attacks against computer software and hardware, and cyber-enabled crime, which encompasses "traditional" crimes that are committed over the Internet.
https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime

Types of Cybercrime:

- **MALWARE —** A category of cyber threats which include Trojan horses, viruses, and worms. These are software that are designed to cause damage to a computer or network. Malware is often used to steal information from individuals or businesses.
  https://techterms.com/definition/malware
- **RANSOMWARE —** A type of malware that prevents users from accessing their system or data until they pay a ransom to regain access.
  https://techterms.com/definition/ransomware
- **PASSWORD ATTACK —** A cyber-attack in which an attacker tries to crack a user's password to gain access to a computer or network. Attackers use programs that may employ a variety of methods to guess passwords.
  https://www.maketecheasier.com/how-password-cracking-works/
- **PHISHING —** Scammers use fraudulent communications – such as email or text – or a fake website to get people to share personal information such as usernames, passwords, credit card details, or Social Security numbers.
  https://techterms.com/definition/phishing
- **DENIAL-OF-SERVICE ATTACKS —** Attackers overload a machine or network by flooding the target with data or traffic, resulting in legitimate traffic being prevented from visiting or using the targeted machine or network. Reasons for these sorts of attacks include disruption or even extortion.
  https://techterms.com/definition/denial_of_service
- **SQL INJECTION ATTACK —** The insertion of a SQL query (a query that programmers use as a language to request and hold data from and for a database) that are covertly injected into an entry field for execution. These insertions may allow attackers to read sensitive data, execute administration operations, or issue commands to the operating system.
  https://www.owasp.org/index.php/SQL_Injection
- **CROSS-SITE SCRIPTING —** A type of injection in which an attacker takes advantage of security vulnerabilities and inserts malicious scripts (a list of executable commands) into web pages. Such insertions can be used to access cookies, session tokens, or other sensitive information retained by the browser and used with that site, or even rewrite the content of the web page.
  https://www.owasp.org/index.php/Cross-site_Scripting_(XSS) https://techterms.com/definition/script
- **SESSION HIJACKING AND MAN-IN-THE-MIDDLE ATTACKS —** An attacker intercepts and relays data sent between two parties, impersonating both sides of the communication. The attacker may alter the communication between the two parties or simply monitor and steal information being sent between the two, such as account numbers and passwords. ***https://www.tomsguide.com/us/man-in-the-middle-attack,news-17755.html***

GENERAL DATA PROTECTION REGULATION (GDPR)

The European Union's (EU) GDPR implements stronger protections for the personal data of citizens of EU member countries and affects any company processing this data. Personal data includes any information that can identify an individual. Even data that has been anonymized or encrypted but can be re-identified with a person is considered personal data.

In collecting data, companies need to explicitly outline the purpose for which they are gathering the information and they should limit their collection to only data that is necessary for those purposes. They also must gain consent before gathering the information and take appropriate measures to keep this data secure as they work with it.

On June 28, 2018, California adopted a digital privacy law of its own which in some ways closely resembles the EU's GDPR. The California Consumer Privacy Act of 2018 (CCPA) will go into effect at the start of 2020.

The information provided here is for general information purposes. We recommend consulting a lawyer for any legal advice regarding GDPR and CCPA compliance.

GDPR:

- *https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN*
- *https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en*
- *https://www.eugdpr.org/*
- *https://www.logmeininc.com/gdpr/what-is-gdpr*
- *https://www.ibm.com/data-responsibility/gdpr/*
- *https://www.itgovernance.co.uk/blog/gdpr-how-the-definition-of-personal-data-will-change/*

CA:

- *https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375*
- *https://www.insurancejournal.com/news/west/2018/07/03/494203.htm*