The Role of Intermediaries in Placing Cyber Risk

Brokers Play a Fundamental Role in Completing the Cyber Jigsaw Puzzle

CyberCube

www.cybcube.com

According to a recent EY survey, just one-third of organizations surveyed thought they had adequate cyber coverage to meet their true exposure to cyber risk. Why is this the case?

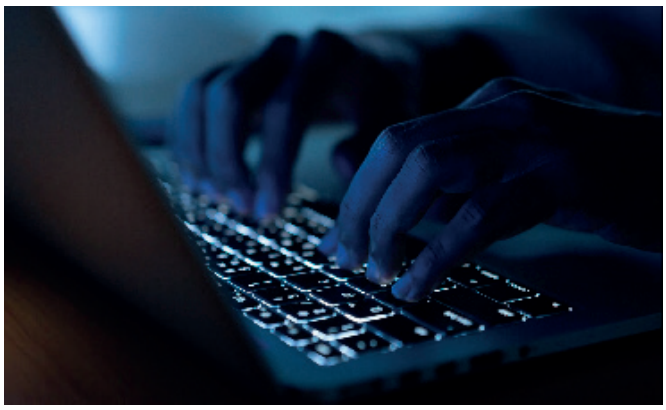
With the wealth of data available to companies and their insurer partners, there should be enough information to tailor specific insurance cover to any organizations' needs. However, upon deeper analysis, there are several structural factors across the market that contribute to this inefficiency and under-protection of corporations.

CyberCube - partnering with leading institutions throughout the (re)insurance and brokerage ecosystem - has identified three factors that hinder growth:

(1) InfoSec and Risk Management functions within a company are often different/siloed and do not always or entirely understand each other's language

(2) When making cyber insurance decisions, cyber is often a relatively small-ticket item receiving very little time and attention as part of the overall risk management purchase process

(3) Differences between cyber policy languages make this a shifting problem that is hard to understand/quantify in absolute terms



Given these factors, this report highlights four understandings and opportunities that can help brokers thrive in this rapidly changing market environment:

(1) Brokers are trusted advisors when it comes to cyber insurance, not cyber security

(2) Understanding exposure is only half the battle, mapping exposure to coverages and policy terms is where brokers' value shines

(3) Helping carriers get to "yes"

(4) Standalone cyber is only part of a well-built insurance program

We do recognize the differences in exposure, risk management approaches and resources between small and large policyholders. Brokers must adapt their advisory techniques, according to their client's characteristics. Most of our findings in this paper apply to both small and large insureds, however, nuances will still exist according to client size and industry.

Challenge: InfoSec and Risk Management functions within a company are often separate and do not always understand each other's language

There is often a disconnect between people in an organization focusing on Information Security (InfoSec) and those considering risk management and insurance. This is especially true for small and medium-sized enterprises, where one or both of these roles may not exist. Not all businesses, for example, have a dedicated individual with a budget responsible for InfoSec, or risk management. In particular, smaller companies do not always have the resources to fully protect themselves or develop a mature and formalized InfoSec or Risk Management program. When it comes to insurance purchasing, this means that a broker has to quickly teach their clients about cyber security risk, cyber insurance, or both.

[1] The EY Global Information Security Survey (2018–19)

Challenge: When making cyber insurance decisions, cyber is often a relatively small-ticket item receiving very little time and attention as part of the overall risk management purchase process

Companies tend to buy cyber insurance as part of a larger insurance program spend, of which cyber insurance plays only a smaller part. For reference, the average spend on cyber insurance for a small company can range from a few hundred dollars to a few thousand. Although this makes sense for the relative magnitude of risk and precedent, the relative cost often presents a challenge when it comes to educating clients about - and placing - cyber insurance.

Cyber risk may look different from company to company but, as a whole, is embedded in every operation that utilizes or relies upon computing or the Internet. The nature of cyber risk, however, is rather complex and requires a fundamental understanding of the underlying exposure (network security, endpoint security, resiliency, data, people and process) and how it relates to various perils such as those of data theft, ransomware, network outage, among others.

These concepts can be difficult to understand at face value, but are exponentially more difficult to explain when given only a limited amount of time on a limited number of slides within a renewal proposal deck or a new business Request for Proposal.

Challenge: Differences between cyber policy languages make this a shifting problem that is hard to understand/ quantify in absolute terms

Participation in the cyber insurance market has evolved considerably over the past two decades. There are an increasing number of markets in the space, each of which has its own proprietary forms. Unlike more traditional and compulsory commercial insurance lines of business, cyber is still treated as a discretionary spend and does not rely upon market standard ISO language. Insurance carriers have their own naming conventions and frame their policies to cover the risks and terms in a manner they are most comfortable with.

Sifting through all of the options and comparing policy language and coverage agreements has become a specialty in itself. Moreover, cyber policies evolve rapidly relative to other lines of insurance, with insurance carriers refreshing their policy forms and coverage offering sometimes annually. Specialists are needed to understand this shifting landscape and how to best pair and map nuanced language to an already technical and disjointed understanding of cyber risk exposure.

A challenge and opportunity for the modern broker

Although these market forces may seem like barriers to the sustained growth of cyber insurance adoption, several leading brokerages have proven that this paradigm presents opportunities for brokers to add a new layer of value-added service. These new opportunities differ in practice, but all stem from the underlying theme that cyber risk presents a unique opportunity for brokers to become trusted advisors helping corporations navigate the complexities of understanding and successfully insure this ubiquitous exposure.

(1) Brokers are trusted advisors when it comes to cyber insurance, not cyber security

Although brokers may find tools that scan networks and uncover vulnerabilities, these findings tend to be complex and can often put a client in a defensive mindset that can become unproductive to the conversation. Rather than focusing on the technical nature of security and exposure, brokers are uniquely positioned to help their clients understand how categories of cyber exposure map to insurable losses, and what steps a company can take to mitigate or transfer exposure for these complex risks. Within this context, historical anecdotes will only carry so far, and insureds will look to brokers for figures and estimates on how to size and structure appropriate cover.

" Brokers are uniquely positioned to help their clients understand how categories of cyber exposure map to insurable losses, and what steps a company can take to mitigate or transfer exposure to these complex risks. "

(2) Understanding exposure is only half the battle, mapping exposure to coverages and policy terms is where brokers' value shines

Standalone cyber policies in the market are designed to address a number of core cyber-related risks that a company may face. However, these products do not necessarily cover all risks and can have gaps that may or may not be addressed in other policies, such as a property policy. Insurance brokers are uniquely positioned to bridge the gap by leveraging their relationships with insurance carrier partners to deliver new, fit for purpose solutions to address both existing and emerging risks associated with cyber exposure. This can be as simple as requesting a carrier's standard endorsements to coverage (such as for an amended acquisition threshold), or can get more nuanced and tailored with manuscripted language (such as for policy language addressing a unique company parent structure or network oversight responsibility).

(3) Helping carriers get to "yes"

As the intermediary, brokers are positioned to represent their client's risk to underwriters, and the underwriters' quotes to their clients. This presents brokers with a challenge to balance a fair portrayal of risk while attaining the best outcome for their client. This also presents an opportunity, however, given the state of the market, and efficacy of their best underwriting relationships.

Underwriters are concerned with balancing the profit and loss of their portfolios, but market conditions have opened up the floodgates for more production-oriented

underwriters as the cyber market is looking to grow. Given these conditions, the technically equipped brokers can feed this appetite for growth by helping underwriting partners get comfortable with the risk with less interruption. Understanding the view of both their client and the underwriter can maximize the efficiency in the process, striking mutually beneficial deals for both parties.

(4) Standalone cyber is only part of a well-built insurance program

Companies face multiple cyber and technology-related exposures, some of which can be triggered by the same event. Given the expanse of policy language in the market, knowing how each policy responds and which coverage agreements would be triggered requires a more experienced and specialized hand. Further complicating the issue, the standalone cyber insurance market has yet to evolve into an all-risk solution. Brokers have to know where one policy ends and another begins, as well as which gaps in coverage exist between different lines of business for a given insured, even when they are assessing policies from the same carrier.

There is an enormous opportunity for brokers to play a pivotal role in facilitating collaboration across multiple lines of insurance cover. This can sometimes take the form of crafting an endorsement for a standalone cyber policy, but may also mean working in collaboration with other lines of business.

Cyber focused brokers are asked to liaise with other lines of business both internally at their brokerage, but also externally with underwriters in other lines of business. Addressing and finding solutions for all of the gaps in all of the policies is not the end-all be-all for brokers. Sometimes, understanding the limitations of an insurance program, and outlining the cost-benefit analysis for that gap is the solution. Having the right tools to know where that line needs to be drawn and putting financial value on both the cost of covering the exposure and the explicit cost of the exposure itself should be the new norm for informed insurance purchasing decisions.

Does Size Matter?

- The risk of a small or large company often looks very different even though they are exposed to many of the same threats. Whereas larger companies may have dedicated roles for risk management and information security functions, smaller companies do not always have the same resources, and roles can be spread thin.
- Additionally, smaller companies encounter resource restraints, both financially (access to capital, competing demands on expenditure) and human (ability to attract talent with InfoSec expertise). It can be difficult for them to develop a mature InfoSec program.
- New coverage of large-scale cyber attacks also contribute to deepening the divide. Smaller companies often feel disenfranchised by hearing of the perils of a larger company, even though they may face the same risks. It is important to educate smaller companies on their own vulnerabilities to similar attacks.
- Regardless of the size of the company, brokers are set to play an increasingly important role in the cyber risk ecosystem. Whether dealing with a large or small client, they maintain the role of trusted advisor, and are one of the first parties to talk to a company about its exposure. Secondly, they are often already entrenched within a customer's business and have a comprehensive understanding of their risk profile. Thirdly, they can bring tools to encompass both technology and the risk management approach. Finally, they have access to and relationships with a breadth of risk transfer options. Considering each of these in aggregate, they are primely positioned to facilitate broader adoption of cyber risk transfer policies.

Concluding Thoughts

Notwithstanding the structural challenges, highlighted above, that brokerages must consider when building out a cyber insurance practice, the ever growing importance of technology across the economy presents a unique opportunity for brokers to deliver an increasing level of value to their clients. Brokerages have the unique opportunity to marry their fundamental understanding of insurable cyber risk and exposure with their core strengths of relationships across the insurance landscape and their in-depth understanding of the policy coverage landscape. Combining these strategic strengths will position brokerages to be indispensable value added business partners for years to come.

CyberCube delivers data-driven cyber risk analytics, developed specifically for the insurance industry.

The combined power of its unique data, multi-disciplinary analytics and cloud based technology helps with insurance placement, underwriting selection and portfolio management optimization.

CyberCube's deep bench of experts from data science, security, threat intelligence, actuarial science, software engineering and insurance build tools by selecting the best sources of data and curating it into data sets to identify early indicators of risks and build a forward-looking view of them.

CyberCube has launched a new product for brokers, Broking Manager, that facilitates quick and efficient client insight for both generalist and cyber specialist brokers. Broking Manager empowers brokers to instantly quantify cyber financial risk for millions of companies, while providing rich information to help brokers articulate their client's cyber exposure.

For more information, visit www.cybcube.com.

Authors

Oren Schetrit, Director of Product Management

John Anderson, Client Services Manager

Yvette Essen, Head of Content & Communications

United States

CyberCube Analytics
58 Maiden Lane
3rd Floor
San Francisco CA94108

Email: info@cybcube.com

United Kingdom

CyberCube Analytics
51 Eastcheap
1st floor
London EC3M 1JP

Estonia

CyberCube Analytics
Metro Plaza
Viru Väljak 2
3rd floor
10111 Tallinn

CyberCube

www.cybcube.com