Technology

TIME TO TEAM

Insurers see strong growth in writing cybersecurity coverage for businesses, but the real prize will go to those insurers that successfully join forces with IT security firms to create more value for their corporate clients.

by Lucy Pilko, Michael Coden and Michael Schachtner

With their other commercial insurance segments struggling to grow, many carriers (about 60 in the United States alone) are seeking to grow sales in the cyber insurance market. That's not surprising. The emerging sector promises real growth in gross written premiums and high profitability given the limited claims received so far.

Insurers will limit their ability to ride the cybersecurity wave, however, if they apply their usual go-to-market approaches. Yes, of course the rising tide of cybersecurity spending—on IT solutions and also legal and public relations counsel—will lift those selling cyber insurance. The real upside, however, will go to the insurers that find ways to successfully join forces with IT security firms.

Pilko

Schachtner

Coden

Contributors **Lucy Pilko** and **Michael Schachtner** are with the insurance practice at The Boston Consulting Group, where Pilko is a partner and managing director and Schachtner is a principal. Contributor **Michael Coden** is the head of cybersecurity at Platinion, a wholly owned subsidiary of BCG. They can be reached at *pilko.lucy@bcg.com*, *schachtner.michael@bcg.com* and *coden.michael@bcgplatinion.com.*

Why? Put simply, insurers have a "business impact" mentality. They are uniquely able to quantify the business cost of cyberattacks and the value of various cybersecurity solutions. Collaborating with IT firms, insurers can provide businesses with quantitative, outcomes-based ways to better understand, manage and mitigate cyberrisk. Insurers' claims data is as valuable to IT firms as the IT firms' data on attacks and defense solutions is to the ability of insurers to precisely price risk.

The first insurers to do this successfully will capture hefty shares of a surging market—and do so profitably—because they'll be better able to select and price risk. Strategically, they will have seized the high ground in corporate cybersecurity as the only ones able to give executive management and boards the insights they need to deal with the threats.

Understanding the Opportunity

Corporate cyberrisk is the subject of numerous articles, conferences, speeches, working panels and task forces. It now looms large on corporate agendas. The Allianz Risk Barometer ranked it as one of 2016's top three global risks for businesses. Regulation is also raising the ante. Next year the European Union rolls out its General Data Protection Regulation, billed as the most important change in data privacy regulation in 20 years.

Businesses, however, are struggling with cyberrisk. Nobody wants to be the subject of the next news headline; every corporation wants to have and hold onto the confidence of its investors and customers. Yet questions abound about the IT vulnerabilities and the probabilities of different types of attacks, as well as where attack prevention ends and consequence management and resilience planning begin.

There is little clarity about what IT solutions work where, or about what role cyber insurance can play in managing risk. Indeed, many companies forgo available cyber insurance policies on the grounds that they are too expensive and it's unclear what they cover, according to the Department of Homeland Security.

Protecting a business against cybercrime is a new challenge for many boards. Many organizations don't feel they are equipped with the tools to manage cyberrisks with the same confidence they bring to managing other risks. A recent survey by the National Association of Corporate Directors found only 19% of respondents believe their boards have a basic understanding of cybersecurity risks. In many organizations, top executives and board members still believe that cybersecurity is only an IT issue.

By themselves, IT firms can provide some of the input that boards and executive teams need to be more confident about how they tackle cyberrisk. Their focus, appropriately, is on technical risk. But by teaming with insurers that have amassed claims data, they can do much more to fully answer the kinds of questions dogging decision-makers today.

A Win-Win Approach

By working together, IT firms and insurers can benefit each other and their clients based on what each party has to offer and what it needs. For example:

- **Insurers can use claims data to pinpoint where data breaches have the greatest business impact.** Insurance firms have a unique edge: the ability to identify and quantify the impact of a successful cyberattack. They can provide hard evidence that not all attacks have

Insurers **must begin reaching out to IT firms** to convince them of how much more **they can do together**.

the same consequences. For instance, the theft of a company's customer data can hurt its brand—at least in the short term—whereas a denial-of-service attack on supply-chain operations will cause immediate financial damage due to business interruption. Additionally, claims data can flag the cost-effectiveness of IT firms' solutions—which tools and techniques provided the best overall returns in reducing the impact of each type of attack. Such data can enable IT firms to build stronger business cases. Although they still sell mainly to IT professionals—chief information officers, information security leaders and others—now they must talk in terms of value and return on investment at least as much as cost and technical features. Today's top IT executives are wired for business benefits, and so are the business leaders with whom they make more and more of their IT sourcing decisions.

- **IT companies can share technology detail.** Typically, IT firms can share details on cybersecurity and the level and intensity of attacks, which systems were affected and so on. They also know from a performance standpoint which technologies are most effective in preventing and mitigating attacks. Armed with such information, insurers can better update their underwriting models, accurately price premiums, proactively reduce their clients' risk exposures and understand aggregation risk. For example, a number of companies are providing cybersecurity rating information–a kind of credit-rating agency for cybersecurity risk–and some leading insurers already are experimenting with this approach to support their underwriting decisions. Working closely with IT firms, carriers can also gain insights into new technologies, enabling them to better plan their own new products.
- **Together, insurers and IT firms can help companies get the highest ROI on cybersecurity solutions.** For all of its uncertainties and urgencies, cybersecurity is not immune to budget constraints, like every other business initiative. Of the funds earmarked for cybersecurity, some will go to tech companies and some to insurers. By sharing cost, tech data and claims data, an insurer-IT partnership can give companies the facts they need to see where they can get better risk protection for a given level of spending—the best mix of IT solutions and cyber insurance for their needs. Some companies may find they can achieve acceptable levels of risk with less technology and more insurance; with others, it may be the reverse. The data will help to make things clear.

Acknowledging the Hurdles

So how practical is it for carriers to collaborate with IT security providers? How can the head of commercial insurance begin to sort through the crowds of giant IT companies—the IBMs and Symantecs and RSAs—not to mention the many small specialists and innovative tech start-ups? How practical is it not to do so when growth in the industry is so elusive? Putting it another way, the critical question that insurers should be addressing is: Where and how can my company participate in preventing and mitigating cyberrisk in ways that enable us to capture lasting advantage?

Insurers must begin reaching out to IT firms to convince them of how much more they can do together. It won't be easy, given that cyber insurance and IT firms are competing for the same slice of their client's budget. However, by cooperating, insurers and IT firms will provide greater value and impact to customers, earning their trust, thereby developing long-term relationships, rather than fighting over their share of today's pie.

Articulating the insurer's case cannot be a job for the head of commercial insurance alone; he or she will lean heavily on the claims group. After all, the claims data and what it conveys is what the insurer brings to the table. The risk-modeling organization will also have valuable input—as will the pricing group. One way to start is with the insurer's information security officer who could be the one to connect with the product leader at the IT firms.

Action Needed Now

This is a time for insurers to act. Cyber insurance offers a bright gleam of growth in an otherwise overcast commercial insurance market. Yes, demand will grow as the cybersecurity sector expands, but right now, there is a brilliant opportunity to capture first-mover advantage by linking up with IT firms.

Already, some well-known insurance providers are exploring such moves. Before long, one or two providers will crack the code on the partnerships with tech firms that more fully enable client companies to understand, manage and mitigate the risks of cyberattacks.

Will your firm be among those leaders? BR