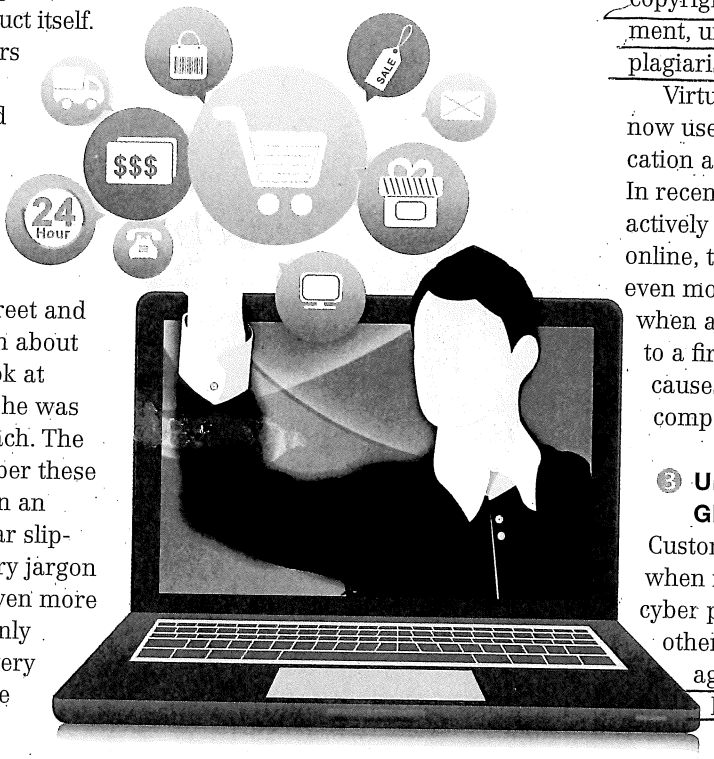
4 Tips to Sell Cyber to Small and Midsized Businesses

BY LISA DOHERTY, TODD CUSANO

CYBER LIABILITY insurance is growing by leaps and bounds—as fast as EPLI by some comparisons but in a fraction of the time. According to online information security provider Symantec, businesses of all size were a potential target for attackers in 2012.

The largest growth area for targeted attacks—comprising 31 percent of all attacks last year—was with businesses having fewer than 250 employees. This represensts a huge opportunity for agents and brokers to sell cyber protection to small and midsized businesses.

Yet cyber insurance is still a relatively new concept that suffers from a lack of standardization in language, coverage and endorsements, along with the confusing nature of the product itself. So as you approach customers in these markets regarding cyber coverage, keep in mind the following four points.



1 MAKE IT SIMPLE AND RELEVANT

If you ran across a potential customer on Main Street and stumbled into a conversation about insurance, he'd probably look at you sideways when asked if he was concerned about a data breach. The very mention of anything cyber these days often leads people down an uncomfortable and unfamiliar slippery path. Relying on industry jargon makes cyber coverage feel even more removed and seem like it's only for high-tech companies or very large firms, which couldn't be further from the truth.

Use simple terms and scenarios to describe data breach/privacy insurance. For example, if you start by asking clients whether they have any personally identifiable information (PII) on their customers or employees and if they have concerns about what would happen if it got out—not because of some hacker from China but rather a disgruntled employee, a frequent occurrence these days—you'll likely get their attention. If you talk about the problems caused if sensitive company data was made public—from financials to salaries—they'll probably lean in even closer.

Most businesses with any employees have PII in some form or another, making it an excellent starting point for discussing cyber protection. All firms with payroll or 401(k) plans have Social Security numbers. If they offer health insurance and medical benefits, even more sensitive information is on hand that needs to be protected.

2 REMIND THAT COVERAGE EXTENDS TO MEDIA LIABILITY

Data breach/privacy policies typically include media liability coverage, a huge plus for many businesses. Virtually anything a company or its employee does gathering and distributing information to the public via a website or other communication (email, social media, desktop publishing, etc.) is covered against claims, including defamation, libel, invasion of privacy, copyright and trademark infringement, unfair competition, piracy, and plagiarism.

Virtually every business in America now uses these methods of communication and thus has media exposure. In recent years, with more companies actively dialoguing with consumers online, this type of coverage is proving even more valuable. For example, when a customer posts something to a firm's social media page that causes injury to a third party, the company can be liable.

3 UNDERSTAND THE GRAY AREAS

Customers are frequently confused when it comes to understanding cyber protection compared with other insurances. Cyber coverages can combine third-party liability coverages with first-

CONTINUED ON P. 18

CONTINUED FROM P. 16

party coverages. Take the case of a breach: The policy will cover the liability incurred as a result of damages to the breached parties, as well as the business interruption from the downtime the firm suffers as a result of the breach. Some cyber products incorporate E&O; others do not. As the agent or broker, it's important to clearly understand the differences, determine the appropriate exposures and needed coverages, and educate your customers.

For example, a software developer needs a technology E&O policy to cover liabilities that arise from providing software products and services. On the other hand, local retailers, or even insurance agencies, do not have a technology E&O exposure, but exposures related to acquiring, storing, and transmitting customer data, typically credit card information and other PII. So the local retailer or insurance agency needs a data breach/privacy policy. The differences are clear.

But the line between the two blurs when a technology company that creates tech products or services also stores and transmits customer data. In this case, the business needs both technology E&O and data breach/privacy coverage, which it can purchase via two separate policies or with a technology E&O policy with built-in data breach/privacy coverage.

Businesses that use a third party or cloud vendor that stores the data are still responsible in the case of a data breach. Some businesses mistakenly believe that their property policy's business interruption coverage will kick in as a result of a data breach, but those policies typically exclude outages caused by computer hackers. If you're comfortable talking to your customers about business interruption in the context of property loss, data breach/privacy insurance is essentially business interruption in the context of an IT issue.

4 MAKE THE CASE FOR BENEFITS BEYOND INSURANCE COVERAGE

People think of insurance as repayment after the fact: If your home burns down, you'll get the funds to cover the damages and rebuild. Data breach/privacy insurance obviously has the component of paying a company's liability following a breach, but the right policy will also cover other essentials for the small to middle market customer who might not have the time or resources to understand proper risk control. Although every step taken is important, simple efforts such as firewalls will provide little protection in the face of an employee error, rogue employee, or lost laptops, tablets, and smartphones.

Imagine the recovery of a firm that makes one call to the first responder to coordinate risk mitigation and crisis management versus a firm that after a breach has to begin the process of identifying and retaining the legal, technology and public relations experts needed to manage the crisis. Weeks of valuable time would be lost in the second scenario.

So cyber coverage is not as simple as, "Here's $600,000 because your house burned down." It addresses what happened, where the hacker went, how to avoid being sued, and how to mitigate the tide of damage to your overall reputation. And if you are sued, in addition to paying for that liability, the coverage will minimize the impact of the lawsuit and damages to third parties.

Explain to potential customers that having the right data breach/privacy policy could effectively provide them with a team of world-class consultants on retainer.

Lisa Doherty is president of Business Risk Partners. Todd Cusano is E&O Project Manager for Business Risk Partners.