Digital Defenders

Cyber insurance products are quickly evolving to cover a widening range of threats and sources.

by Dennis Gorski

Agents and brokers who are looking for this year's sweet spot of opportunity and growth will find it in cyberspace insurance.

The niche market for cyber is rapidly becoming a mainstream offering, experts say, and its awareness among commercial prospects is the highest of any insurance product. The media has brought cyber front-and-center, and agents, brokers and other producers clearly stand to gain.

Although the massive Target Corp. data breach of last holiday season was the shock wave that sent cyber's profile to the fore, it's been a growing line for the past several years, said Phil Harvey, principal of Venture Insurance Programs, a West Chester, Pa.-based program administrator. He has 40 years of insurance experience, the first 20 in retail. "It's a brand new industry going forward. It's in vogue," he said.

Helping to drive cyber protection's explosive growth, he said, is mobile technology. "We're in a period of mobile breaches. IPads, smartphones and tablets have increased the ability for information to be stolen. All the information we think is safe, there's a big bridge it's crossing before it gets [to the receiving site]. That's where the interference occurs. Most people have these mobile devices 'open.' They're not secure."

A few years ago, data breaches might have involved a mortgage company's laptop disappearing from a taxicab. But the threat has evolved in scale and sophistication, especially from overseas hackers. "Things really have heated up over the last two years in cyber protection," he noted. "Preventive measures are a big play for agents and brokers."

Harvey said the era of big-time hacking began with the health care industry. "The health care industry was the first to be attacked because it had the most confidential information," he said. "It's a large industry that was extremely vulnerable because of its size and its uniqueness, and it contained a lot of information that wasn't necessarily secure—personal, financial and secret data. And lots of people had open access to it."

Another big issue in cyber insurance is legislation—sometimes coming from federal elected officials and agencies, but more likely state-based. "Each state is trying to establish its own protocol for rules, regulations and carrying out of reforms," Harvey explained. "It's difficult because very few companies do business in one state." Even small companies can be global because they don't need branch offices; everything can be done digitally, he added.

Although Target Corp.'s data breach was stunning in scope, it won't be the last, according to Laura Johnson, vice president at Euclid Managers, a privately held underwriting manager in Kansas City, Mo. Nor is cyber breach limited to big-box retailers, she pointed out. Big business, banks, governments, educational and military installations and nonprofits are all victims of hackers, malware, credit card skimmers and theft.

Johnson referred to a recent post by the Privacy Rights Clearinghouse, a 501(c)(3) organization, citing 55 commercial breaches from January through March 27, 2014. Victims ran the gamut, from a gas station in rural Ohio to the Internal Revenue Service to American Express.

When asked if Target's hacking episode drove a spike in cyber insurance, her answer was an emphatic "yes." Harvey added: "Most insureds that respond to [the Target breach] do so primarily to hedge their bets. They've been thinking about buying cyber but haven't been convinced that something could happen. They think, 'It won't happen to me because I run the best business in America.' For someone like Target to be fooled has shown me a lot about how vulnerable we all are."

According to a June 2013 study co-authored by the Ponemon Institute and Symantec, human error and systems glitches caused nearly two-thirds of data breaches globally in 2012. What's more, malicious or

criminal attacks are the most costly, averaging $157 per compromised record.

Today, with breaches potentially affecting millions of unaware customers, seven-, and eight-figure jury awards for liabilities and penalties could become common. One jury, in Indiana, recently found Walgreens liable for $1.4 million after a pharmacist-employee breached a single customer's personal health record and showed it to her husband. The victim was his former girlfriend, court records revealed.

That's why cyber, which covers soft liability costs and hidden risks, is a smart play for businesses, Harvey said. "No one thinks [their risk] could ever be that bad, but they can put you out of business, especially if you're not a public company."

"I think when consumers see a merchant breach, they figure it's the merchant's problem," Harvey noted. "But it's not the merchant's problem; it's the consumers' problem on how they use the media, their credit cards, their handheld devices, their iPads. A lot of it is carelessness."

Agents and brokers who are very well-educated about cyber—"schooled up on it," in Harvey's words—and have risk management experience, should find numerous leads. Prospective insureds "need someone who's going to bring the posse together," he said, and that has to be the agent or broker, not the company attorney or even the insurance company. The posse, he explained, includes the client's IT team, its CFO and its counsel, because they'll all be involved at the time of claim.

"It's a good pre-empt to have them 'up' on how coverage works and where exposures lie." BR

Selling Commercial Cyber Liability Insurance

Who should have it: Any industry, professional corporation or nonprofit that does banking, credit card transactions or personal records accretion or transferals.

Purpose: To protect insureds against exposures when communicating or conducting business online, including email, social media and the Internet. Policies are tailored to the business' specific risks and needs. Coverage is available for internally or externally launched data loss; business interruption; liability for privacy breaches; crisis and reputation management; cyber extortion and identity theft, or transmission of malware and viruses.

Product type: Becoming more of an admitted-lines product, although many cyber products are written as excess and surplus policies because of their versatility. Can be stand-alone or bolt-on. Often found in comprehensive package products. First-party coverage covers IT forensics, notifications, credit monitoring, crisis management and PR. Third-party coverage is for legal liability, defense and settlement of customers' claims, lawsuits, possible class action, regulatory actions and fines, payment card industry fines and remediation coverage. **Note:** For a detailed examination of cyber- and data-breach policies please go to "Two of a Kind" on page 28.

Exclusions: Crime indemnity may pick up certain elements but excludes data or info that's transmitted. Unless purchased as options, online media content, cyber business interruption, cyber extortion, hacker damage (the cost to rebuild network), and various Internet website events (among others) are excluded.

Limits: Average deductible of $2,500 to $5,000 will buy several million dollars' worth of basic coverage for small businesses and entities. Very large corporations doing $1 billion or more in revenue will have "super limits" as high as $100 million with deductibles starting at $250,000 from branded carriers. Self-retention at this level is the norm. Reinsurers cover such risks with quota sharing.

Capacity: Market is well capitalized.

Key Considerations:

- Cyber coverage parallels many features of kidnap and ransom cover, particularly in the realm of investigation of the breach, the use of insurance company "go teams" to take over the matter, and discovery costs, public relations and reputation repair expenses.
- "Cloud" cyber cover is available as an E&S product. But many issues concerning digital storage in the cloud need resolution, including its borderless nature and which entities actually control its digital contents.
- Policies have discovery periods and reporting periods, which can vary.
- Insureds can buy optional 1-, 2- or 3-year tail coverage, which provides basically runoff coverage during that period. The secret to this coverage, especially for those that have never had this cover before, is to negotiate the best retrospective date they can—to cover previous events that haven't come to light yet.
- A good agent or broker will recommend the insured bring in outside consultants for IT screenings to pinpoint places where the client may be vulnerable. It's much less expensive than being exploited by hackers later.
- The cyber "target" is always moving quickly; mobile devices today have capabilities and apps that weren't available 12 months ago. All these new exposures offer new opportunities for agents, brokers and carriers.