CYBER THREATS in the INSURANCE MARKET AND CAPTIVES

By Karrie Hyatt

Large-scale cyber attacks dominate the news, while more and more businesses are experiencing a large range of incidents. Insurance products are available to help companies withstand these attacks, but according to several new reports, many companies are not investing in cyber-related insurance due to expensive premiums and gaps in available products. Captives are filling in those gaps and, often times, are more competitively priced in comparison to the traditional market.

The Cyber Threat

According to the Internet Security Threat Report (ISTR) published annually by Symantec, the overall number of computer system breaches was lower in 2016 than 2014, falling by more than 300. However, the number of identities exposed during each breach rose in average from 805,000 per breach to 927,000. While successful cyber attacks are becoming less frequent, those that do succeed often cause more damage.

But it isn't just big businesses that are being targeted. In a report from the National Cyber Security Alliance published during last October's National Cyber Security Awareness Month, in 2015 43% of cyber attacks targeted small business, while during the same time 82% of small business owners said that they were not targets for attacks.

One of the fastest growing forms of cyber attack are ransomware attacks. On May 12, the world was rocked by a massive cyber attack in the form of a ransomware email that affected computer systems in at least 100 countries. Ransomware attacks, which have been gaining in frequency, is when malware, usually sent by email and unwittingly opened by an employee, is used to take over another computer system or network and then hold its data hostage.

The benefit to cyber thieves is that it is easier and more profitable to hold data ransom than to steal it. So much so that in Verizon's 2017 Data Breach Investigations Report (DBIR), they have a section titled, "Ransom Notes are the Most Profitable Form of Writing." The report says that ransomware attacks were some of the earliest types of hacking, but have seen an uptick in usage due to the anonymity of Bit Coin payments and off-the-shelf style hacks that can easily be exploited.

In Symantec's ISTR, between 2015 and 2016 the number of detections of ransomware attacks rose 123,176 to 463,841, with the types of hacking software going from 30 samples to more than 100. Most of the time, ransomware thieves demand small amounts of money as an incentive for companies whose systems are being held captive to pay up right away. However, as these attacks become more pervasive and emboldened, the average ransom amount rose to $1,077 in 2016 from $294 in 2015, according to the ISTR.

In 2016, 73% of cyber attacks were financially motivated, as stated in Verizon's DBIR. 66% of breaches were made due to malicious email attachments. Phishing—infecting a computer through an email attachment or via a link to steal data—is still the most common way that companies and individuals are attacked. However, ransomware and pretexting have started to gain ground on phishing attacks. Pretexting is often aimed at financial companies

and is highly targeted, unlike ransomware. Pretexting involves an outside party sending a specialized communication to a party with control over finances or data—often impersonating an executive or vendor—and getting them to transfer large amounts of money or reveal important information. This attack is most often achieved through email interaction.

Cyber attacks that target the human factor is far more likely to happen than hack often portrayed on TV. Cyber criminals find it much easier to infiltrate a company's systems by exploiting an unwary employee than taking the time and energy to break through a company's firewalls and other security measures.

The Insurance Answer

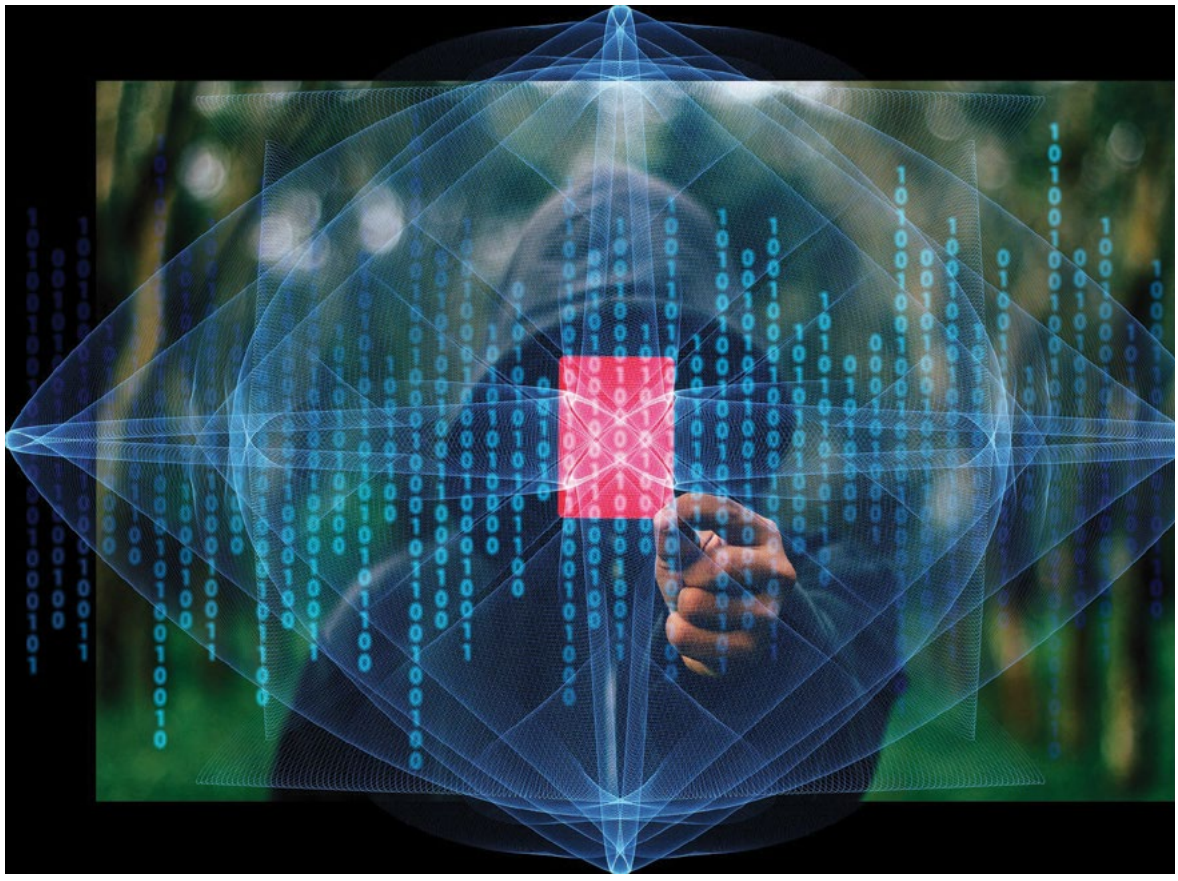
Another recent report sponsored by Aon Risk Solutions and independently conducted by Ponemon Institute LLC is the 2017 North America Cyber Risk Transfer Comparison Report. It found that while most companies fear a cyber attack, the uptake of cyber-related insurance is still well below property, plant and equipment (PP&E) coverage. According to the report, "The probability of any particular building burning down is significantly lower than one percent (1%). However, most organizations spend much more on fire-insurance premiums than on cyber insurance despite stating in their publicly disclosed documents that a majority of the organization's value is attributed to intangible assets."

The report is based on a survey of nearly 20,000 individuals who work with their company's cyber risk and enterprise risk management activities. Some of the highlighted findings of the study were that: 89% believe that cyber liability is in the top ten risks for their company; 56% experienced a business disruption due to a cyber attack during the previous two years; information assets are underinsured against theft or destruction; and companies, knowing the risk, are still reluctant to purchase cyber insurance.

While the findings indicate that companies believe information assets to be slightly higher in value than PP&E, information assets are underinsured by comparison. "On average, approximately 62% of PP&E assets are covered by insurance…. In contrast, an average of 16% of information assets are covered by insurance." However, companies who self-insure are 59% more likely to have information asset coverage.

More than half the respondents (64%) believe that cyber security threats will increase in the coming years, with only 11% believing that it will decrease. Cyber risks, which are more likely to come to fruition than PP&E risks, are also far more likely to cause significant business interruption in comparison to PP&E. Yet still companies are slow to get adequate coverage.

The main reasons, according to the report, for not purchasing cyber coverage are: premiums are too expensive; coverage is inadequate based on exposure; too many exclusions, restriction and uninsurable risks; and property and casualty policies are sufficient.



Guardian® in sync Stop Loss

When evaluating stop loss carriers, just look at the numbers.

Looking for assurance that Guardian Stop Loss Insurance will protect you against catastrophic claims and higher than expected medical plan usage? Our numbers speak for themselves:

Only 2–3 days to turn around claims, whether $10K or $10M[1]

155 years of financial stability, so you know we'll be there when you need us

98 (out of 100) score from Comdex, making us one of the most highly rated insurers[2]

Visit www.guardiananytime.com/stoploss

GUARDIAN® LIFE | DENTAL | VISION | DISABILITY | ABSENCE | SUPPLEMENTAL HEALTH | STOP LOSS | ASO

GuardianAnytime.com

The Guardian Life Insurance Company of America®, 7 Hanover Square, New York, NY 10004. GUARDIAN® and the GUARDIAN G® logo are registered service marks of The Guardian Life Insurance Company of America and are used with express permission.

[1] Upon receipt of information from the payer. [2] As of 2/2/2016 and subject to change. Source: Vital Signs. Comdex is a composite of all ratings that a company has received from the major rating agencies (A.M. Best, Standard & Poor's, Moody's, and Fitch).

Guardian's Stop Loss Insurance is underwritten and issued by The Guardian Life Insurance Company of America, New York, NY. Policy limitations and exclusions apply. Optional riders and/or features may incur additional costs. Financial information concerning The Guardian Life Insurance Company of America as of December 31, 2015 on a statutory basis: Admitted Assets = $48.1 Billion; Liabilities = $42.0 Billion (including $37.0 Billion of Reserves); and Surplus = $6.1 Billion. Policy Form #GP-1-SL-13. File # 2016-21397 Exp. 8/17

The Captive Factor

The reasons that companies are not purchasing cyber coverage, as cited in the Ponemon Institute's report, can be addressed by captive insurance companies. The risks that companies find hard to insure or that are underinsured can often be attended to through a captive.

Due to the flexibility of coverage that captives can offer, companies have the ability to customize the coverage to suit their needs. Health care facilities, financial companies, and government departments will all have specialized needs when it comes to cyber security threats and need insurance coverage to reflect those differences. Traditional commercial markets, while stepping up to offer a variety of products to meet cyber attacks, don't have the flexibility to fine tune coverage to each companies' needs.

Captives can also be used to cover risks that are not available in the commercial market, by either entirely insuring the risk or by offering excess coverage where it is underinsured. Captives can also insure reputation and cyber as a package, as well as other interconnected risks, that might be overlooked in the wider insurance marketplace.

While much of the pricing in the insurance market has been declining in 2016 and 2017, the two exceptions are auto and cyber. For cyber insurance, the commercial pricing has been increasing for several reasons. Cyber is still considered an emerging product and can still be too changeable to be anything but a challenge to underwriters. The increased pricing is also due to the increase in severity and frequency of incidents, as well as the higher amount of losses. Again, this is something that captives can address with their flexibility.

Exceptional. Period.*

* Actual member comments about their surgery through the BridgeHealth program.

We connect plan members with top-quality surgical care for 20% to 40% less than a typical PPO plan. **Contact us and learn why great care doesn't have to mean great cost.**

(855) 456-9064 | www.bridgehealth.com

BridgeHealth™

The primary obstacle for companies turning to captives to provide cyber coverage is coming up with the funding to establish the reserves needed to fund future losses. As the costs of major cyber attacks rise, it may be hard for captives to anticipate the reserves they will need to pay out claims. Equally, because of the range of potential damages—from a few hundred in a ransomware attack to potentially millions in the case of exposed customer data in a large breach—deductibles tend to be high for both captive and traditional markets. This might also rule out captives as a valid alternative for any but very large companies.

Companies without the proper reserves might find a solution by forming a rent-a-captive or establishing a cell captive. Smaller companies who are interested in the solutions captives can offer to comprehensive cyber coverage can experience many benefits of a fully-owned captive through a cell captive without the large reserves needed to start a pure captive. ■

Karrie Hyatt is a freelance writer who has been involved in the captive industry for more than ten years. More information about her work can be found at: www.karriehyatt.com.