Bloomberg BNA

Daily Report for Executives™

Insurance

Insurers Are Using New Tool To Assess Companies' Cybersecurity Risk

Cybersecurity risk ratings are giving insurers a new way to assess the hazards of covering current and potential customers.

Leading the way in cybersecurity scoring is BitSight Technologies, a Cambridge, Mass.-based company that has been assigning continuously evolving cyber scores on a real time basis for about a-year-and-a-half.

''We produce a rating that is similar to a credit score or a FICO-like score for security,'' Jacob Olcott, BitSight vice president of business development, told Bloomberg BNA.

Companies hoping to cushion the financial blow from a data breach are driving sales of cyberinsurance, which has become one of the fastest-growing insurance products. The market is worth more than $2 billion in gross written premiums, according to an October Insurance Information Institute white paper that cited Marsh LLC, an insurance brokerage.

And the risk of cyber breaches has been steadily increasing in the U.S. From the under-siege financial sector to the health and education industries, cyberattacks now stem from more sources than ever before—such as nation states, terrorists, criminals, activists, external opportunists and company insiders.

Another factor driving companies to purchase cyberinsurance is regulatory—expectations of more government scrutiny and penalties for negligently allowing consumers' private information to be compromised in an attack.

In one such case, St. Louis-based investment adviser R.T. Jones Capital Equities Management, Inc. agreed on Sept. 22 to pay $75,000 to resolve Securities and Exchange Commission allegations that it didn't have mandatory cybersecurity polices in place to prevent a data breach that compromised approximately 100,000 individuals' personal information (*In re R.T. Jones Capital Equities Mgmt., Inc.*, 2015 BL 306149, SEC, Admin. Proc. File No. 3-16827, 9/22/15) (See previous story, 09/23/15).

Evan Wolff, a partner at Crowell & Moring, said that the government can help companies out by getting clear rules on the books sooner rather than later.

''Government can help industry come up with clear standards and best practices, which can allow companies to understand where they can best invest their money,'' said Wolff.

''Government can help industry come up with clear standards and best practices, which can allow companies to understand where they can best invest their money.''

EVAN WOLFF, CROWELL & MORING

Cyber liability policies can help cover costs incurred from a breach, such as regulatory compliance costs, consumer notifications and credit monitoring and/or liability for failing to secure private data, among many other things, the Center for Insurance Policy and Research (CIPR) said. It can even cover the restoration of computer systems lost to a breach.

Keeping Score. More than 60 carriers offer standalone cyberinsurance policies, according to the III white paper. While BitSight currently offers a cybersecurity rating system, Tara Swaminatha, a cybersecurity specialist with law firm DLA Piper, said there are other companies developing similar systems.

Some of the world's largest insurers utilize BitSight, including American International Group, Inc., ACE Group Holdings, Inc., and Liberty Mutual Insurance Co., BitSight said on its website.

BitSight's scoring ranks companies on a scale of 250 (worst) to 900 (best). The cybersecurity ratings, which are updated daily, hinge on two main factors: security events and network configuration.

''Security events represent evidence of successful cyber attacks,'' the company's website says. ''Examples of security events include communication with known botnets, port scanning, malware distribution and malicious e-mail propagation.''

''Configuration information represents how diligent a company is in mitigating risk,'' according to the site. ''Proper email server configuration, for example, can help prevent email related attacks and indicates that a company has implemented good risk management practices.''

BitSight notifies insurers when their customers experience a significant fluctuation in their security score. Insurers can also measure a business's third-party's networks to further assess and monitor a current or potential customer's risk.

''The ratings are based on externally observable incidents that are collectable from around the Internet,'' BitSight's Olcott said. The company's technology allows

Cyberinsurance Is a Growth Industry in the U.S.

As data breaches steadily increase, more companies are turning to cyberinsurance, making it one of the fastest growing insurance products in the U.S. Cyber-liability policies might include one or more of the following types of coverage:

A BNA graphic/cybr03g1

insurers to get a clearer picture of how well a potential client is protecting its computer networks. ''Some insurance companies will use us to monitor their customers,'' he said. ''We provide these ratings in a continuous, real-time basis.''

''What we're actually able to observe are the security outcomes,'' he said.

BitSight is able to analyze the ''bad stuff'' leaving a company's network through the use of sinkholing, a way to reroute, filter and analyze network traffic.

''BitSight obtains the data used for our ratings from our extensive sink holing infrastructure and by incorporating data from other publicly accessible sources,'' the company explained to Bloomberg BNA via a Dec. 3 e-mail.

OneBeacon's Wurzler said that his company had been using BitSight for about a year.

BitSight's cybersecurity rating product ''provides a really good 20,000-foot view,'' Wurzler said. ''Their tool has external sensors looking at weaknesses and vulnerabilities for companies.''

''It's a good preemptive tool,'' he said, adding that OneBeacon was in the process of expanding the use of BitSight's ratings to help OneBeacon agents evaluate the cybersecurity risk of potential and current customers.

  DER ISSN 0148-8155

Many tools are used by insurers to help assess risk, Wurzler said.

"Although the market for cyber liability insurance is off to a good start, it is expected to grow dramatically over time as business gradually becomes more aware that current business policies do not adequately cover cyber risks."

CIPR DOCUMENT

Financial Consequences. ''Although the market for cyber liability insurance is off to a good start, it is expected to grow dramatically over time as business gradually becomes more aware that current business policies do not adequately cover cyber risks,'' according to a CIPR online document updated in September. CIPR is part of the National Association of Insurance Commissioners, which releases model rules for states.

Cyberattack consequences run the gamut from destruction of company computer systems to the theft of a company's consumers' private information. The financial consequences can include:

- interruption of business,
- theft of valuable assets, including customer lists and trade secrets,
- the cost of credit monitoring services for clients affected by a data breach.

Insurers are finding it hard to measure the true actuarial risk of cyberattacks on companies precisely because the effects can be so varied (See previous story, 09/11/15).

In a recent example, Target Corp. agreed on Dec. 2 to pay more than $39 million to banks and credit unions for losses from a 2013 holiday-season data breach that led to the exposure of as many as 40 million payment cards (*In re Target Corp. Customer Data Sec. Breach Litig., D. Minn.*, D. Minn., No. 0:14-md-02522-PAM, 12/2/15) (See previous story, 12/03/15).

One attack could even potentially plunge a company into financial ruin, OneBeacon Technology Insurance President John Wurzler told Bloomberg BNA, Sept. 22.

On the other hand, a company may only have to reset passwords to avoid footing the bill for measures like credit monitoring for a year for each consumer impacted by an attack, as some regulators have recently suggested (See previous story, 10/22/15).

More to the Puzzle. Despite the benefits of a completely automatic scoring system like BitSight's, DLA Piper's Swaminatha said it doesn't cover all the bases and that other companies developing ratings systems may offer a more comprehensive approach.

''It just isn't a complete picture,'' Swaminatha told Bloomberg BNA. ''You could have two companies with the exact same score that have [a] completely different cybersecurity maturity.''

''That's not saying there's a better way to do it now, but it's just maybe 50 percent of the puzzle,'' she said. Still, Swaminatha clarified that, ''I think what BitSight is doing is good.''

She said Bitsight's method is objective and repeatable and that having that kind of measurement is certainly an important component of any cybersecurity test.

There should be versions of the rating system that are more comprehensive, she said.

However, there is a problem with the currently available comprehensive methods. ''There are comprehensive approaches, but none of them are automated,'' Swaminatha said.

Perhaps just as important to companies is that the comprehensive tests are more costly and time-intensive.

Locking Down Third-Party Vendors. While many large companies have strong cybersecurity defenses and protocols in place for their networks, many small ones don't, experts said at a Sept. 10 discussion on cybersecurity at the Center for Strategic and International Studies (CSIS). Many breaches begin in the overlap, usually when large companies use small companies as their suppliers and vendors.

''Companies are as weak as their weakest link,'' Wolff told Bloomberg BNA. In the case of network security, that weakest links can be the smaller, third-party vendors—who may believe they are too small to be targets.

Crowell & Moring works with companies from those that have established solid cybersecurity measures to those taking their first steps, according to Wolff.

"The more information you can have on the partners and networks and vendors of a company, the better you are, the more secure you can be."

EVAN WOLFF, CROWELL & MORING

''The more information you can have on the partners and networks and vendors of a company, the better you are, the more secure you can be,'' Wolff said.

Because large companies may work with a large number of third-party vendors, some insurers are now requiring companies to vet the strength of their vendors' networks systems before guaranteeing the large company with a cyberinsurance policy, the panelist said at the CSIS said.

And insurers aren't the only ones concerned here.

Policy makers and government agencies are taking note of the risk third-party vendors pose to networks, too.

''[I]n a very organic way, third-party vendor risk has become a critical issue for regulators, which is exactly what BitSight is being used for,'' BitSight's Olcott told Bloomberg BNA in November. ''What BitSight has been spending time on recently is educating regulators about best practices in vendor risk management—beyond changing contracts and sending out questionnaires, how organizations can continuously monitor their vendors.'' Recent examples of government attention to third-party cybersecurity is a Nov. 9 letter the New York State Department sent to other financial regulators lay-

ing out plans to issue new regulations that would include third-party risk management requirements, Olcott said.

Olcott pointed to another example of government interest in third-party breaches via the Department of Defense's placement of new cybersecurity rules on its prime contractors and subcontractors requiring that they manage their own risk and risk of their third parties.

This is where the cybersecurity scoring comes back into the mix, helping any company gain an overview of its vendors' and perspective partners' cyber health. ''There's a lot of interest in the scoring process,'' Crowell & Moring's Wolff said. ''[I]t's the next sort of logical area that companies will need to use to manage their supply chain and evaluate their partners.''

When asked if the use of ratings would probably increase as more companies seek cyberinsurance policies, Wolff said: ''I think we're going to see that trend continue.'' Wolff said that the cyberinsurance policies are going to get more popular.

Cyber insurance policies have ''gone from an exotic policy to something that is very common,'' Wolff said. ''I think we're going to see an increase in the number of polices being written and I think we're going to see an increase in the information exchanged between companies and insurers.''

BY BRANDON ROSS

To contact the reporter on this story: Brandon Ross in Washington at bross@bna.com

To contact the editor responsible for this story: Heather Rothman at hrothman@bna.com

  DER ISSN 0148-8155