ADVISEN
Insurance Intelligence®

CYBER INSURANCE UNDERWRITING: A HIGH-TECH, EVOLVING DISCIPLINE

November 2014

Sponsored by:

BITSIGHT

CYBER INSURANCE UNDERWRITING: A HIGH-TECH, EVOLVING DISCIPLINE

As cyber risk became better understood over the last few decades, insurance buyers found some protection against associated losses in various policies, including professional liability, crime, property and general liability.

Introduction

Despite a staggering rise in the exposures faced by global businesses from cyber attack, data theft or privacy violations, the insurance industry remains well capitalized and willing to supply substantial cover to organizations in the form of cyber insurance.

Advisen's buyer penetration index shows a five-fold increase in cyber insurance purchases from 2006 to 2013 – a growth rate many emerging sectors would be proud of!

Many insurance carriers in the cyber market consider themselves to be experts in underwriting corporate cyber exposures, having specialized in the area since its inception in the late-1990's and early 2000's.

Underwriters use various tools to assess the cyber exposures of prospective clients and offer guidance on how best to mitigate those risks and secure the best available terms from the insurance community for risk transfer.

This paper will assess how the cyber market has developed and will look at some of the tools carriers are adopting to better assess corporation's cyber preparedness in the underwriting process.

The cyber insurance market today

As cyber risk became better understood over the last few decades, insurance buyers found some protection against associated losses in various policies, including professional liability, crime, property and general liability.

The stand-alone cyber insurance market, which continues to attract additional underwriters, has grown to 50 or 60 insurers from the US, Bermuda and London markets, according to Parisi and Foster.

The level and availability of that protection, however, has evolved dramatically over the past decade. For example, insurers are moving toward excluding cyber risk coverage from general liability policies.

Stand-alone cyber risk insurance provides the most comprehensive cover for the litany of potential damages that data breach victim organizations suffer, according to insurance broker Robert Parisi, the New York-based managing director and leader of the network security & privacy practice at Marsh USA.

Those policies typically offer a menu of coverages. Insurance buyers can find coverage for their costs to:

- Investigate the data security breach incident
- Restore lost data
- Harden the breached data security system against future attacks
- Notify customers and clients that their personal information has been compromised
- Provide credit-monitoring services to customers and clients
- Retain crisis management experts
- Defend against subsequent regulatory actions and consumer and investor lawsuits
- Respond to cyber extortion

Some policies also cover lost revenues, subject to prescribed deductibles, waiting periods or sublimits, Peter Foster, Boston-based executive vice president-FINEX North America at Willis noted.

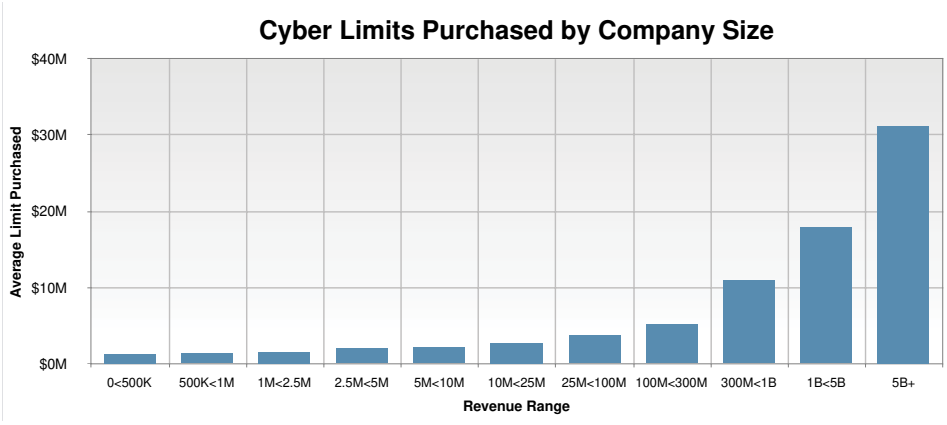
The stand-alone cyber insurance market, which continues to attract additional underwriters, has grown to 50 or 60 insurers from the US, Bermuda and London markets, according to Parisi and Foster. Among those underwriters, about three-dozen write both primary and excess coverage, and about two-dozen write on only an excess basis, Foster says.

The brokers estimate that buyers can easily layer together up to $200 million of cyber insurance limits. However, Foster notes that one account has pulled together $350 million of coverage.

There also are efforts to pull together much greater protection for insurance buyers. For example, Foster notes that two separate accounts are pursuing $500 million of limits, “and it’s a distinct possibility” they will succeed. Meanwhile, Marsh has made arrangements for a group of insurers to provide larger risks up to $600 million of limits with a $100 million self-insured retention. That product is designed for accounts seeking only catastrophe coverage, Parisi observes.

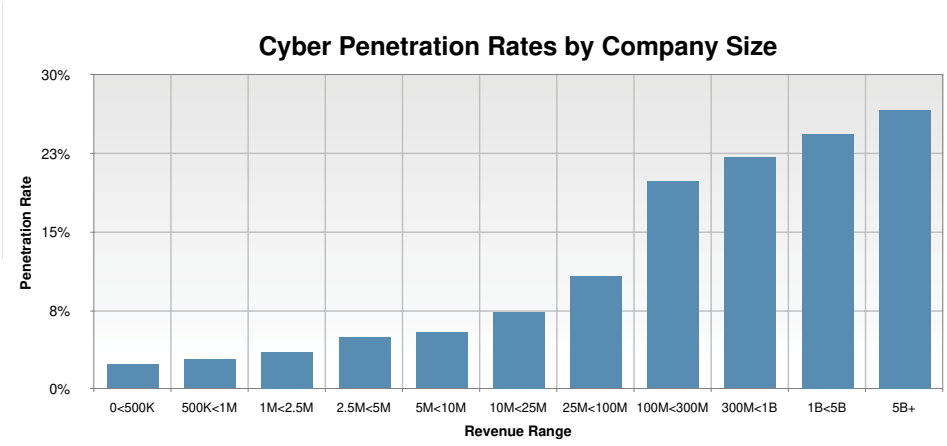
While Target and other well-publicized breaches have raised awareness, experts note that other factors also are driving more and more companies to develop response plans.

The average amount of limits that policyholders purchase, however, is much smaller, according to Advisen's Jim Blinn. Smaller companies purchase about $1 million of limits, while large companies purchase about $32.5 million of limits.



Source: Advisen

And despite providing ample capacity and offering flat to slightly lower rates to most accounts, the cyber risk insurance market is far from reaching its potential market penetration, according to Blinn of Advisen. At just more than $1 billion of gross written premiums annually, insurers could be writing five times as much at today's rates, according to Blinn.



Source: Advisen

Insurers can find market opportunities at companies at every size. Companies with $5 billion or more of annual revenue currently account for insurers' deepest market-segment penetration rate: 25.9 percent. Among mid-sized companies—those with $100 million to $1 billion of annual revenue, market penetration rates range from 17.5 percent to 20.5 percent. Insurers' penetration rate is the lowest—in the single digits—among companies with $25 million or less of revenue.

Companies can identify risks and adopt risk management leading practices to ease the process of finding the right cover at the right price.

Assessing risks

The task of the cyber insurance underwriter is to adequately assess the exposures faced by its clients and to determine the extent to which those risks are being mitigated in the risk management process.

Once assessed, the underwriter can select the appropriate levels of cover and insurance pricing.

Underwriters have a number of tools available to them to underwrite those risks: from client-completed application forms, online risk assessment tools, or third party technology.

Companies can identify risks and adopt risk management leading practices to ease the process of finding the right cover at the right price. The insurance industry is moving towards insisting upon this enterprise level of risk mitigation before it issues cyber cover.

Indeed, broker Willis' FINEX division is offering an accreditation to clients who pass a risk assessment test online. The Cyber-ATLAS tool includes an eLearning tool feature. On completion of the assessment, corporations will qualify for Cyber-ATLAS accreditation that can lead to "significant discounts on a cyber liability insurance policy", the firm said.

Many brokers and insurers offer technical services such as cyber risk assessment tools, accreditation to receive insurance discounts, penetration testing, external validation of cyber risk preparedness, cyber rating tools etc.

And insurance executives maintain that they are adhering to strict underwriting standards to evaluate the nature of prospective policyholders' cyber risk.

"We're not making underwriting decisions without the technology to back them up," says Matthew Prevost, the Philadelphia-based vice president and privacy and technology product line manager at ACE USA.

Traditional underwriting tools, including the written application form, are becoming less relevant to an enterprise-wide risk such as cyber.

A recent survey carried out by reinsurer PartnerRe noted that brokers and underwriters felt that the cumbersome application was an obstacle to selling insurance. One respondent noted

As in technology, if you're not evolving from an underwriting perspective, you're behind

that "supplemental applications can be pretty extensive" and another said "many clients will not be able to provide all the additional documentation for the underwriting process". Therefore carriers are beginning to adopt more analytics and technology to assess risks. Just as organizations' technologies and their attendant cyber risk evolves, so does the insurance underwriting process, according to market executives. "As in technology, if you're not evolving from an underwriting perspective, you're behind," ACE's Prevost asserts.

Harnessing data

In the last decade, the insurance industry as a whole has used new technologies and high-speed computers to analyze data at speeds unimaginable before. Catastrophe exposures, longer life spans and health care increase the need for modeling and analytics. The same is true for as the new emerging risks including cyber and climate change.

Data is arguably the most important asset in the insurance industry. Models are only as good as the weakest point in the data. The more analytics and big data become mainstream strategies, the more attention needs to be paid to data quality

"Data is arguably the most important asset in the insurance industry. Models are only as good as the weakest point in the data. The more analytics and big data become mainstream strategies, the more attention needs to be paid to data quality," according to consultancy EY in a 2014 paper: "*Mitigating cyber risk for insurers*".

Risk modeling has had a major effect on the underwriting process for property catastrophe risks, for example, bringing objective, verifiable underwriting discipline to the class of business. Is data on cyber incidents as robust as it is in other fields?

Over the last five years, the most significant development in the evolution of cyber risk underwriting has been the increased amount of data on the risk, according to underwriters.

"We're using more strategic analytics to get at what trends are happening before we are hit with it," says Scott Schleicher, the Washington, DC-based cyber underwriting manager in XL Group's new cyber and technology unit. "We are starting to get more data - internally and externally," Schleicher says.

"As we grow our data - to pinpoint trends, higher risk industries, etc. - we are getting more information to make better judgment calls," which also allows insurers "to price cyber coverages more appropriately", according to Schleicher.

M&A activity and financial results may correlate with the budgetary commitment a CISO can make to data security

Insurers examine a variety of factors when underwriting cyber risk. Whether it is a stand-alone cyber risk policy that provides the broadest insurance protection available or a professional liability, crime or property policy, insurers try to understand the same factors about the insurance buyer's cyber risk. However, the evaluation process is more rigorous for stand-alone coverage, notes Ken Goldstein, vice president and worldwide cyber security and media liability manager at Chubb Group of Insurance Cos.

Underwriters want to know the volume and type of data that prospective policyholders retain, and that typically is a function of their industry and the size of that company. "Different industries retain different kinds of information that can be breached. And different sized companies hold on to different quantities of information," Schleicher explains.

With such information, ACE generates trend metrics on various types of information, gleaned from data inside as well as outside of ACE. For example, merger and acquisition activity and financial results in a given industry may correlate with the pressures a chief information security officer might face and the budgetary commitment an insurance buyer can make to data security.

Underwriters also might want to see how that data is protected from both unauthorized access and negligent disclosure that could result, for example, when a laptop computer or smartphone containing sensitive data is lost or stolen. They look for data security details such as whether data is stored on a company server or with a cloud provider, system firewalls, data encryption, the ability to remotely wipe data from stolen devices, how quickly a former employee's system access is revoked, system-penetration detection capabilities and compliance with the latest PCI Security Standards for credit card transactions.

Some measures, however, such as system-penetration detection, are used by only "the most sophisticated" insurance buyers, such as financial institutions, XL's Schleicher notes.

In addition, vendor management controls are critical, Goldstein says. Insurers examine not only the expertise of vendors the insurance buyer has retained to provide system security but also the system restrictions the buyer has imposed on these vendors to prevent them from accessing data they do not need. The importance of those restrictions is underscored by the massive Target data security breach. Data thieves accessed the company's data security system with codes stolen from a heating and air conditioning vendor that had serviced many of the retailer's stores, according to security blog Krebs on Security.

What we would really like to see is more information on the breaches that are occurring out of the spotlight

ACE reviews the insurance buyer's contracts and the software and technologies it uses and can correlate all of that information to the insurers own claims data. Those vendors would include not only technology companies but also, for example, human resources and payroll software firms, Prevost notes.

Some insurers also review the reports produced by the high-tech vendors that insurance buyers retain to provide data security. Others provide online risk management portals for policyholders. At those sites, insurers offer policyholders guidance on how to maximize their data security.

Brokers as well as insurers rely on technology to model their clients' cyber risks and design a risk-financing program for them.

For example, Willis developed the Privacy Risk Insurance Strategy Model—or PRISM. Accessing a database of thousands of data breaches over recent years, the software tool projects the likelihood of an organization suffering a breach and the amount of the resulting loss.

The model calculates the annual frequency for each organization based on the number of breaches within that organization's industry group, the universe of organizations within that industry group that could have had such breaches and the relative quality of each organization's controls. After running *Monte Carlo* simulation using the frequency data and cost-of-breach data from two independent research firms, PRISM generates an uninsured loss probability distribution specific to the client's industry sector. Then, using a metric that incorporates the client's risk appetite and cost of capital, the tool overlays various risk-financing structures to identify the optimal combination of limit, retention and premium for the client.

The future of cyber underwriting

Underwriting tools devised in-house by brokers and carriers, have their limitations, however, and independent vendors have begun to launch new tools designed to offer a third-party perspective on a client's exposures.

"What we would really like to see is more information on the breaches that are occurring out of the spotlight," XL's Schleicher told Advisen. "And there are many of them. There are hundreds of other breaches that are small: How it occurred, who did what - it's all

In addition to these new tools, there is potential for significant further development in the use of technology in underwriting cyber insurance.

information that's valuable to us. With more data mining, we can gather the information we need to have the right information across industries, regions, and sizes of businesses".

Schleicher added that "all businesses are vulnerable to a breach, and the more information we have about the variety of incidents, where they came from, etc., will be ever more valuable to writing the risk and developing the cyber coverages that can help businesses effectively address the risk".

In answer to that call, information Security firm, BitSight, has launched Security Ratings for Cyber Insurance, a "first-of-its-kind" solution for underwriters and brokers to model cyber risk.

BitSight's security ratings, ranging from 250 to 900, give insurers access to a data-driven measurement in order to quantify the risk and adjust coverage and premium.

The automated service analyzes, rates, and monitors security performance, all from outside the company. Policyholders do not need to provide any information and there is no intrusive testing involved.

"Instead of the questionnaires and interviews, insurers will have the ability to view their entire books security performance over the last 12 months and compare," said Ira Scharf, chief strategy officer at BitSight. "Insurers and brokers can average risk and calculate how it has changed over time for a particular company – an insured or an applicant - and compare performance to that company's peers."

Liberty International Underwriters has signed on to use the ratings and other insurers are evaluating the underwriting tool.

In addition to these new tools, there is potential for significant further development in the use of technology in underwriting cyber insurance.

Consulting company EY said that it is possible to mathematically create a "cyber index" in the same manner that weather and stock market indices appear in the macroeconomic models representing market risk exposure correlation to other enterprise risks.

Topping the wish list is a means to determine how truly exposed data is when vendors have access to it in the supply chain.

"This cyber index could be created from the data patterns of the cyber catastrophe models and other data and then used as a threshold to trigger a data breach claims process following notification of a data breach," the EY report said.

Another third party aid to cyber underwriting would be to create a data-scoring rating mechanism for global ratings agencies, EY said.

Insurers "can then take the output of these newly emerging data-rating agencies to compare the internal risk models of the various third parties being used", EY said. "The companies using data integrity standards will receive a higher rating, as they have mitigation in place in line with international standards and leading practices".

Wish list

Advisen asked insurance executives what tools they could use to aid in assessing insurance buyers' risks.

Topping the wish list for Chubb's Goldstein is a means to determine how truly exposed data is when vendors have access to it in the supply chain. While insurers currently can gauge how well policyholders manage vendors' access to data, they do not have a clear picture of whether those vendors sub-contract with other vendors, the access those subcontractors have to the data and how robust those subcontractors' data security systems are.

Willis' Foster wants a tool that would measure the business interruption loss that a manufacturer or retailer would sustain as a result of a supply chain disruption due to a cyber attack.

ACE's Prevost says underwriting will continue to evolve as does the technology that clients adopt, such as computer-chip-imbedded credit cards and mobile wallets, which allows consumers to pay for items at a store register with the touch of a button on their smartphones. He notes that ACE's underwriting team works with the insurer's own data security and technology group to "understand the threat environment better."

Some data security experts, however, foresee a fundamental shift in data protection that would far more effectively thwart cyber criminals, making organizations of all sizes far better risks for insurers.

The cyber insurance market is a dynamic environment, characterized by rapid evolution in cover, services, limits and pricing of today's cyber risks.

Currently, perimeter security is the focus of data protection. That terminology dates back to the early days of computing and electronic data storage, before the widespread use of networking on the Internet. In those days, data could be stolen only by removing rather conspicuous, bulky electronic components from a company's building. Companies could protect their data through traditional perimeter security measures, such as property fencing, locked doors and guards.

In the age of networking, with data now movable over the ether, those traditional perimeters have given way to methods such as server firewalls and data encryption.

The drawback with perimeter security today is that it allows a company to control data only when it is within the company's perimeter, or on its own systems, explains data security consultant Dan Kruger, chief executive officer of Absio Corp.

But today, if data "has any value at all, it has to be shared with somebody outside" of that perimeter, Kruger says. That means data could be protected from cyber thieves far better if data owners could maintain control of the data wherever it is.

This so-called data-centric control is a matter of software engineering: designing the digital objects that hold data, not to release it unless those attempting to access it have the necessary codes and the permission of the data owner, Kruger explains.

Conclusion

The cyber insurance market is a dynamic environment, characterized by rapid evolution in cover, services, limits and pricing of today's cyber risks.

And as the exposures faced by corporations today increase exponentially, the greatest challenge for the insurance industry is to keep up with developments and provide meaningful solutions at the right price.

Therefore, the underwriting process is undergoing change – in the amount of data harnessed and utilized in the risk rating process, as well as the use of new technologies to offer different views of policyholder's risk management strategies.

The future of the cyber insurance marketplace depends on a robust, transparent underwriting process, backed by meaningful data. The market today is responding creatively to these challenges and laying the foundation for a solid future ahead. ■