Why CISOs Should Embrace Their Cyber Insurer

6 Steps to Start Working Together Today

Symantec Cyber Insurance

Cyber Security risk management is undergoing one of the most important shifts in recent memory; however, this shift is not being driven by the information security industry. Cyber Insurance is emerging as a critical new risk management tool for companies and, according to Fitch, it is the fastest growing segment in property/casualty insurance. But what does this mean for information security professionals?

When surveyed, corporate clients and insurance brokers from Allianz recently rated cyber risk as the third most important peril that corporates were facing. This placed cyber risk above traditionally insured risks such as fire, natural catastrophes and even above macroeconomic developments and changes in legislation and so it is no wonder that cyber insurance is experiencing such explosive growth. Risk managers are driving the purchase of cyber insurance policies to cover the tremendous losses that can be incurred from cyber attacks but what is the role of information security professional?

Too often, CISOs and the information security team have cursory engagement with their cyber insurer. This is bad for the CISO, bad for their insurer and ultimately, bad for the cyber resilience of their company. 40% of information security professionals with titles like Chief Information Security Officer (CISO) don't fully understand the "characteristics and limits of the company's cyber insurance coverage," according to a study conducted by SANS. In the same study, it was reported that only 14% of insurance broker respondents thought that CISOs understand and value the insurance well. That should not be the case. In general, information security professionals and their insurers are on the same team, with the same objective - making companies more resilient to cyber attacks.

This article lays out 6 ways CISOs should start engaging with their corporate risk managers, brokers and insurance carriers today.

1. Understand what cyber insurance coverage your company has already purchased

Only 64% of SANS respondents that are covered either by third-party coverage or are self-insured know how their organization obtains that coverage. [1]

Coverage for cyber risk is complicated by the fact that it can be purchased as a standalone cover or embedded into other lines of insurance such as property, general liability or crime policies. Knowing what is and is not covered is an important first step and will often require engagement with the risk management department and the company's broker.

Many companies have notification requirements to get their insurer involved in case of a breach. At worst, information security departments should be aware of the policy and its requirements. At best, insurers will have a seen a large number of breaches and can be a tremendous resource working through everything from coordinating vendors to offering advice and mobilizing response teams.

2. Get involved with risk managers in the cyber insurance purchase process and in insurance renewals

Majority (88%) of brokers report that their clients engage senior security management (CISOs) in insurance purchasing decisions, but only 15% report that CISOs have "much" influence over those decisions. [1]

Engagement should be more than perfunctorily providing information in an underwriting questionnaire and joining a group conference call. Engaging with the information security organization can lead to better premiums by allowing the company to "tell its story" and display the security culture that exists in the organization. In one instance, a top 3 broker reported that two airlines with broadly similar cyber security postures achieved a 30% differential in the cyber insurance pricing, which was attributed in substantial part to the confidence projected by a highly engaged cyber security team in the purchase process and the "culture of security" that CISO was able to portray.

As an information security professional, you are also an important party in the insurer selection process. For example, a Fortune 2000 technology company was using a leading Managed Security Service provider to

[1] SANS: https://www.sans.org/reading-room/whitepapers/analyst/bridging-insurance-infosec-gap-2016-cyber-insurance-survey-37062

oversee its cyber security. However, the vendor was not on the insurer's incident response panel. This meant that in the event of a breach, the company would not be reimbursed for the additional breach response costs incurred with the managed security provider. Without engagement from the CISO, the company could have purchased a policy that prohibited their most trusted security partner from responding in a breach, which had the potential to slow down the speed of response in a crisis.

3. Proactively offer up information in the underwriting process – holding back information will often lead to worse outcomes for your company

Over 70 companies currently offer some sort of cyber insurance cover, however insufficient information in an underwriting application is a major reason why insurers do not participate in a broker's request for proposals.

Providing security information to an insurer is often misunderstood as a game of 'gotchas'. In a market of supply and demand, having fewer insurers offer up rates because you haven't provided sufficient information can hurt your ability to get the best rates and build sufficiently high towers of cover. Insurers want to avoid "bad risks", so they will be on the lookout for practices that they deem risky however in general providing more information will enable more carriers to quote insurance. Think of it like an auction of a piece of property. You want as many bidders as possible but providing only piecemeal information creates uncertainty and lowers participation.

Providing information about strong security practices is best, however skipping questions or providing partial answers will lead to insurers assuming the worst as underwriters only have the information that is provided by the company. CISOs should not be afraid to provide supplemental information, explanations on why a security practice isn't in place and why a control is only partially implemented. Without such explanations, a carrier may assume the worst or simply not participate, which leads to lower towers of cover and potentially worse pricing and terms for the client company.

This does not mean that a CISO needs to share absolutely everything about the proprietary security operations and plans of the organization in the same way the CFO of a publicly listed company would not share every last detail of a company's projected financials in an earnings call. For example, sharing plans to remediate security deficiencies is important, however, given the uncertainties of implementation an organization may want to hold back from sharing highly granular plans with detailed roll-out dates that would likely be reviewed again at the time of insurance renewal. A CISO should provide enough information for underwriters to make informed decisions about risk, which is typically far more than what is provided today.

Research from Advisen shows that insurance brokers are frustrated by divergent and sometimes conflicting expectations from underwriters, due to the market's rapid state of flux and a wide variation in understanding of the criteria to be used to assessing an organization's cyber risk posture. Cyber underwriting is an evolving discipline that is slowly improving as the industry matures and adopts new data modeling and software tools to make better risk decisions. In the meantime, engaging proactively in the underwriting process and having patience for the questions insurers are asking is an important step.

4. Information Security personnel should engage in a transparent dialogue about what security they don't currently have and take steps to remediate those gaps

Some carriers will offer a premium reduction of 10-20% if additional security is purchased - without engaging with the information security department, companies lose this leverage with insurers, especially if they were going to make the purchase anyway.

Insurers are on the hook for costs associated with a cyber break and are willing to spend money making the client safer. It makes sense for an insurer to cover the costs of a data breach wishes to incentivize companies to purchase leading data loss prevention software to protect

that sensitive data. Similarly, if a company is insuring against ransomware, which is almost exclusively delivered via email, the implementation of email security filtering is an important addition and could be subsidized by the carrier. Companies are leaving money on the table by not understanding that their insurer isn't trying to "catch them out" but can be a real partner in creating a more resilient cyber security program.

Carriers will often include free, trial, or discounted cyber security services to their clients but this requires engagement from the information security team. Looking for security awareness training for employees? In some cases, insurers will pay for material from a cyber security company like Symantec. Need a new incident response planning? You may have never had a breach but insurers deal with them on a weekly basis and may even pay for a team to run a tabletop exercise with you.

5. Security professionals shouldn't avoid talking about prior breaches with their insurers and should bring them up proactively to talk about how they are planning for the next one

Insurers will often use tools and databases to understand the security history of a company and may even know about breaches from several years ago that the information security team is unaware of. For example, Advisen contains a breach database of 35,000 cases.

To make matters worse, sometimes it is the insurer informing the risk manager of previous breaches that he or she was not aware of. This doesn't inspire confidence in the insurer who could be on the hook for tens of millions of dollars in the event of a claim. Security professionals should be deeply engaged with risk management and insurance buyers.

6. Proactively identify and quantify your insurance needs in conjunction with your broker and risk manager

It's critical for security professionals to take this engagement one step further and proactively drive the identification of cyber insurance needs. Sarah Stephens, from JLT, comments "CISOs should be a critical part of crafting exactly what customized cover their company needs to purchase. Starting from a risk-threat-scenario point of view rather than a 'what will the market offer' view can be the key to making rather than reacting to the market."

"Starting from a risk-threat-scenario point of view rather than a 'what will the market offer' view can be the key to making rather than reacting to the market"

– Sarah Stephens, JLT Specialty Limited

The cyber insurance market is still relatively nascent. Policies don't tend to be standard between insurance carriers and brokers, who are still wrapping their arms around how to advise on cyber insurance purchase decisions. Some brokers will have tools and frameworks to help identify and quantify needs but ultimately information security professionals, who are closest to the risk, can be instrumental in identifying what should be covered and at what level.

Summary

As cyber insurance emerges as an important new line of insurance, partnership between risk managers, information security professional, technology vendors and insurers becomes increasingly important to improving cyber resilience. Security professionals should not see insurers or underwriters as an unwelcome intrusion or 'big brother' second-guessing a company's security protocols but rather as a partner protecting the firm's assets, sometimes with tens of millions of dollars of the insurers money on the line. It's time for CISOs and insurers to take one step closer and embrace each other in a united front against cybercrime.

Author: Pascal Millaire, Vice President and General Manager of Symantec Cyber Insurance

For global offices and contact numbers, please visit our website.

Symantec Corporation World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA
+ (650) 527 8000
1 (800) 721 3934
www.symantec.com

Follow us on Twitter @SymantecCI

About Symantec:
Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Symantec operates one of the world's largest civilian cyber intelligence networks. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure.

Symantec Cyber Insurance
Symantec Cyber Insurance (www.symantec.com/solutions/insurance) empowers underwriters, portfolio managers and actuaries with underwriting and catastrophe modeling software built for the cyber insurers, incorporating data from the insurance and cyber security communities.