This article has been published in
PLI Current: The Journal of PLI Press, Vol. 2, No. 2,
Spring 2018 (© 2018 Practising Law Institute),
www.pli.edu/PLICurrent.

PLI Current
The Journal of PLI Press
Vol. 2, No. 2, Spring 2018

Cyber Insurance Gone Wrong: Insurance Mistakes That Have Cost Risk Managers Their Jobs

Thomas H. Bentz, Jr.
Holland & Knight

The average tenure of a chief information security officer is just seventeen months according to CIO.com.[1] One reason for CISOs' short tenure is the ever-increasing number of data breaches. But CISOs are not alone in the list of casualties that result after a data breach. Increasingly, risk managers, CFOs, and others responsible for purchasing cyber insurance that is supposed to protect a company in the event of a data breach ("risk managers") are also at risk for losing their jobs.

The unfortunate thing is that, unlike a company's ability to stop a breach, avoiding costly mistakes with your cyber insurance policy is avoidable. The fol-

lowing provides real-life examples of insurance mistakes that resulted in a risk manager losing his or her job. We have also provided some tips to help make sure that you avoid being the next casualty of the cyber war.

Failing to Appreciate the Importance of the Cyber Insurance Application

One of the more common mistakes risk managers make with their cyber policies is failing to understand the importance of the application. The definition of "application" in a cyber policy is important because the application is the foundation for the coverage. If material information is omitted or misstated in the application, it may constitute application fraud and could result in rescission of the policy or a denial of coverage for a claim.

Unfortunately, many cyber applications ask extraordinarily broad and complex questions and expect a risk manager to check a box with a simple "yes" or "no" response. Questions such as "Is the applicant compliant with all applicable data security standards?" or "Is the applicant in compliance with its privacy policy?" are often not so easy to answer with just a yes or no response. However, the potential consequences of a "wrong," partial, or inadequate answer can be devastating.

A cautious risk manager must take care to share the application questions with management, the IT department, and any other relevant group to make sure the answers are 100% accurate. If a yes-or-no response is not adequate, a risk manager must take the time to explain the full answer in attachments to the application. However, since any answer that is not "yes" may result in a limitation of coverage from the underwriter, it is important that the response be narrowly tailored to limit the potential negative impact. For this reason, we strongly suggest that legal counsel be involved in responding to the questions in the application.

Not Understanding Sublimits of Coverage

Cyber policies often come with ten or more coverage grants, each with a "sublimit" of coverage. Most of the grants are described in the main policy form, but the sublimits are described in the declarations page. This can be confusing, especially if there are endorsements that modify either the grants or the sublimits of coverage, which is often the case.

On more than one occasion, a risk manager has failed to recognize the significance of these sublimits of coverage and how they will impact the coverage. In a very common example, an insured secured a $250,000 sublimit of coverage for PCI fines. When the risk manager purchased the first cyber policy, this was "standard," and higher limits were not commonly available from the insurer for this coverage grant. However, just a few years later, higher limits were easily available upon request. Unfortunately, the risk manager did not know this, and not requesting the higher limit ended up costing the company significant amounts that could have been covered by the insurance policy. When this fact was highlighted during the claim process, the risk manager was terminated from his position.

To avoid this costly mistake, a risk manager must ask his or her broker each year whether additional coverage is available for any sublimits of coverage. Because cyber insurance is changing so quickly, things that were not insurable or only insurable at low limits a year ago can sometimes now be fully covered by a cyber policy.

Failing to Know About the Duty to Defend

Most cyber liability policies are written on a "duty to defend" basis. This means that decisions such as which law firm to use, whether and how to defend a claim, and on what terms a claim should be settled are determined by the insurance carrier and not the insured. Although this is fine for some, many companies may be uncomfortable with this arrangement in the event of a large breach or regulatory matter that may determine the future of the company or severely tarnish the company's reputation.

That was certainly the case when one risk manager explained to her board of directors that the company could not use the law firm that the company used to draft and implement its cyber risk policies but, instead, had to use a law firm picked by the insurer that was completely unfamiliar with the company's history or business model. As the chairman of the board put it, "This is a bet-the-company case. We are not going to bet our company's future on a law firm that we have never used or even heard of." When the board realized that using its preferred law firm would mean that the insurer would not pay any of the defense costs incurred in the matter, the risk manager was terminated.

To avoid this situation, risk managers should carefully review the defense arrangements with the board, general counsel's office, and the IT department in advance of a claim. If the company has a specific law firm or vendor that it wants to use, it should negotiate this prior to renewing its coverage. Often, insurance carriers are willing to allow the use of a specific law firm or vendor if the issues is raised at renewal. Underwriters have strong incentives to accommodate such requests; claim adjusters, however, do not.

Failing to Raise Hourly Rate Limits

Some insurers allow their insureds to use "any law firm they want" as long as the firm is "qualified" and its hourly rates are "reasonable and necessary." That may sound attractive, but it is often difficult to find a top service provider that will work for what an insurer considers "reasonable and necessary."

In a recent breach situation, an insured had three quotes from law firms to handle the breach work—the least expensive law firm quoted $600 per hour for the work. The most the insurer would approve as reasonable and necessary was $209 per hour. Since the insured could not find a service provider that would work for $209 per hour, it had to either use the law firm recommended by its insurer or pay the difference between what the insurer was willing to pay and the amount the qualified vendors it found were willing to charge. This left the company with a tab of nearly $400 per hour that was uninsured.

The legal fees for the matter ended up in the millions of dollars, leaving the insured with a hefty portion of the defense costs uninsured. The company blamed the risk manager for the uninsured legal fees because the risk manager failed to inform the board of the issue in advance of the breach and the risk manager failed to negotiate a change to the coverage.

This situation could have been avoided if the risk manager had known about the rate caps and informed the board of the limitation of coverage. As noted above, underwriters are often willing to negotiate on this topic whereas claims adjusters have little incentive to do so.

Failing to Secure Coverage for Social Engineering Fraud

One of the more common and costly mistakes made by risk managers in recent years is the failure to obtain coverage for "voluntary transfers" related to social engineering fraud or phishing attacks.

There are many variations on this scam, but essentially, the CFO receives what appears to be a legitimate email from a client or vendor asking the CFO to wire money to an account. The email often looks completely real and, in fact, is often the result of a hacker having broken into the client's or vendor's system, allowing the hacker to send messages from the client's or vendor's actual email address. Only after wiring the money (often multiple transfers and increasingly larger sums) does the CFO learn that he or she has become a victim of fraud.

Unfortunately, many companies are not covered for this type of loss even if they purchase cyber liability insurance coverage. Most cyber insurers will not cover this loss because it was not the insured's system that was hacked—instead, it was the insured's client's or vendor's system that was breached. Without a breach, there is no covered loss under the policy despite the obvious fraud on the insured.

Adding insult to injury, the typical crime/fidelity bond policy will also not respond because there is no "theft" in a social engineering scam because the insured "voluntarily gave" the money to the scammer. Many crime policies specifically exclude any "voluntary transfer" of money from coverage. This exclusion applies even though the CFO was tricked into wiring the money.

The most frustrating and unfortunate part of this situation (and one reason multiple risk managers have lost their jobs over this issue) is that coverage for this type of social engineering fraud is generally available upon request from most crime policies and some cyber liability insurance policies. Moreover, there is usually only a nominal additional premium required for the coverage.

However, making sure that your cyber policy has at least some coverage for social engineering is not enough. Recently, one cyber insurer has started offering higher limits of coverage for social engineering fraud provided that the insured has and follows a multi-factor authentication process prior to wiring any funds. While this may sound attractive (and many risk managers have purchased this coverage), the reality is that if a company is following a multi-factor authentication process, it is extraordinarily unlikely that the company will be the victim of a social

engineering fraud. In other words, the "extra" coverage only serves to provide the insurer a reason to deny coverage because the company failed to follow the multi-factor authentication process. This can leave the company with even less coverage than if it had not purchased the coverage "enhancement."

Failing to Improve the Retroactive Date

When purchasing cyber liability coverage, it is important to negotiate the retroactive date. Many policies only cover cyberattacks or data breaches that occur after the retroactive date—typically the date that the insured first purchased coverage from the insurer.

However, this may leave an insured without coverage for a network security breach that occurred, but was undetected, before the retroactive date. Since many data breaches go undetected for months or years before the company learns of the problem, purchasing a new cyber policy without full prior-acts coverage may result in a policy that has very little value for the first several months.

Many insurers are willing to provide backdated retroactive dates upon request. However, few insurers will offer the extra coverage unless asked.

Failing to Negotiate the Excess Policies

Most cyber liability insurance programs with more than $10 million in limit will require an excess "follow form" policy. Despite their name, few excess policies truly follow the terms and conditions of the primary insurance policy. Instead, most excess policies will add various terms and conditions that have the potential to significantly impact the overall protection provided by the cyber insurance program of insurance.

Notwithstanding the potential impact that these added terms and conditions may have, excess policies are often wholly neglected. Insureds fail to analyze or negotiate their excess policies for many reasons. Sometimes, they just assume the excess policies are all the same, and they just pick the cheapest one. Often, they just run out of time to deal with the excess policies as the renewal date approaches.

This makes little sense because, once the limit of liability of the primary policy is exhausted, the excess policies will be very relevant to whether a claim will continue to be paid. In fact, in a large insurance program, the excess policies often constitute the vast majority of the limit of coverage.

One risk manager learned this when she discovered that the excess policies in her program would not cover any "sublimited" coverage in the primary policy. Unfortunately, every coverage grant—even those that were sublimited to the full primary policy limit—was labeled as sublimited in the primary policy. This gave the excess policies a reason to deny coverage for the claim and the board a reason to terminate the risk manager.

Bonus Tip: Plan for the GDPR

The EU's General Data Protection Regulation (GDPR) will go into effect on May 25, 2018. The law impacts all businesses that provide goods or services to individuals in the European Union, regardless of whether the business has stores or processes data within the European Union. The maximum fine for not complying with the GDPR is EUR 20 million (roughly USD 23.7 million) or 4% of a company's worldwide revenue (not profit), whichever is greater.

Although cyber insurance can provide protection for fines and penalties, it is not clear whether the current language in many cyber policies will cover the fines and penalties related to the GDPR.

The time to clarify this coverage is now. At least one insurer has provided a specific endorsement to make it clear that its cyber policy will cover any fines or penalties related to the GDPR. Without such an endorsement, a company may find itself uninsured—or at least stuck in a battle with its carrier over coverage. Risk managers that have the foresight to add this coverage before a claim occurs could save their companies millions of dollars. Those risk managers that fail to at least investigate whether the coverage is available may be looking for a new job in the event of a claim.

Conclusion

Cyber insurance is changing rapidly with new policies and coverage grants appearing on a regular basis. Risk managers have the tough job of needing to stay current on new and constantly changing coverage, and keeping their board informed of the coverage that they have. Too often, boards are content simply knowing that they have a policy and the overall limit of coverage they purchase. This is not enough and can prove costly to both the company and the risk manager. Although difficult, a well-informed risk manager can save the company after a cyber breach. Perhaps just as importantly to the risk manager, taking the time to understand and negotiate the company's cyber insurance coverage may just save his or her own job.

Thomas H. Bentz, Jr. practices insurance law with a focus on D&O, cyber and other management liability insurance policies. Mr. Bentz leads Holland & Knight's D&O and management liability insurance team, which provides insight and guidance on ways to improve policy language and helps insureds maximize their possible insurance recovery. Mr. Bentz is the author of the chapters on Directors and Officers Liability Insurance and Cyber Liability Insurance in PLI's Corporate Compliance Answer Book (2018 ed.).

NOTES

1. Scott Hollis, *The Average CISO Tenure Is 17 Months—Don't Be a Statistic!*, CIO (Sept. 17, 2015), www.cio.com/article/2984607/security/the-average-ciso-tenure-is-17-months-don-t-be-a-statistic.html.