Don't Wait Until It's Too Late: Top 10 Recommendations for Negotiating Your Cyber Insurance Policy

By James P. Bobotek

As more and more companies of all sizes ranging across a wide spectrum of industries have been exposed to network and data security breaches in recent years, the market for insurance products dedicated to cover cyber risks has grown just as fast. With policies sold under names like "cyberinsurance," "privacy breach insurance," "media liability insurance" and "network security insurance," the market for this coverage often seems chaotic, with premiums and terms varying dramatically from one insurer to the next.

Unlike more traditional insurance policies that contain very similar terms, conditions and exclusions no matter which insurer issues them, cyber insurance policies are far from uniform. Prior to placing or renewing a cyber policy, it is therefore crucial to understand not only what you are being offered, but also how to negotiate coverage for the risks inherent in your business. Every policy's coverage is different. Before you buy or renew a cyber policy, be sure to review and understand the following guidelines.

1. Buy Only What You Need

Many cyber policies provide an "à la carte" arrangement that includes the option to purchase seven basic coverages. Three of those coverages involve third-party losses: (i) Privacy Notification and Crisis Management Expense; (ii) Regulatory Defense and Penalties; and (iii) Information Security and Privacy Liability. Two involve first-party losses through what are commonly referred to as "time element" coverages: (i) Business Interruption and (ii) Extra Expense. The other two, also first-party related, provide "theft of property" coverages: (i) Data Assets and (ii) Cyber Extortion.

With all the bells and whistles now offered by some insurers, consider the specific risks against which you wish to insure, and whether you really need all of the coverages being offered. Always include notification and crisis management expense coverage, as well as regulatory defense coverage. Time element coverage is also important, especially for small businesses, as lack of income for even a short period may be disastrous.

If an insurer is unwilling to remove an objectionable exclusion or limitation from its policy, then ask your broker to get bids from other insurers. The cyber insurance market is highly competitive, with many insurers currently focused on building market share. This means that one might be willing to provide coverage or terms that another will not.

2. Carefully Vet the Limits of Liability

One of the most important issues in negotiating cyber coverage is determining the appropriate limits of liability. The costs of responding to a data breach can be substantial. In 2014, the average organizational cost of a data breach was approximately $5.8 million. Response costs for breaches involving the loss or theft of personal data were as much as $950 per electronic record. To put that number in context, a data breach involving just 25,000 records—a below-average total—would exhaust a $5 million policy. And if plaintiffs in a class-action suit obtained a judgment under a state statute that imposes $1,000 in damages for each claimant, the judgment alone could consume $25 million of insurance policy limits. Because cyber insurance is relatively inexpensive, you should choose limits of liability in line with your total potential liability exposure in the event of a breach. Your broker should be able to assist you in determining appropriate limits by utilizing its benchmarking databases.

Most cyber policies impose sublimits on some coverages, such as for crisis management expenses, notification costs or regulatory investigations. These sublimits are not always obvious, and they are often inadequate. They should be scrutinized carefully and set realistically. Also make sure that the policy's aggregate limit applicable to all coverages is not less than the total of all sublimits.

3. Obtain Retroactive Coverage

Many cyber policies limit coverage to breaches that occur after a specified "retroactive date." In some, this date is the same as the policy's inception date. This means there may be no coverage provided for claims made due to breaches that occurred before the policy period, even if the insured did not know about the breach when it bought the policy.

Because breaches may go undiscovered for some time before claims are made, insureds should always ask for a retroactive date that is earlier than the inception date. This will ensure that the coverage includes unknown breaches that first occur prior to the policy's inception, but do not manifest themselves until after that date. Insurers do not always offer retroactive coverage unless asked, but it is commonly available for periods of one, two, five or ten years. Some offer unlimited retroactive coverage.

4. Beware of Broadly Worded Exclusions

It is not uncommon to find cyber insurance provisions that contradict the insured's basic purpose in buying the coverage. Sometimes these provisions have been cut from other insurance policy forms and pasted into cyber insurance forms where they do not belong. For example, some policies broadly exclude coverage for any liability arising from a breach of contract. Many insureds collect and store confidential information from customers, patients or business partners pursuant to contracts that require them to maintain the confidentiality of the information. They buy cyber insurance precisely to protect them in case a privacy breach gives rise to damages claims under such confidentiality agreements.

Many insurers, if asked, are willing to modify exclusions to make it clear that they will not bar coverage for claims that go to the core of an insured's business. This is just one of many examples of broadly worded exclusions that need to be reviewed carefully and narrowed to make sure that they will not defeat the reasonable expectations of the insured in buying cyber insurance.

5. Beware of Panel and Consent Provisions

Many cyber policies require that any investigators, consultants or attorneys used by the insured to respond to a claim or potential claim be drawn from a list of professionals that have been pre-approved by the insurer. If you would like your preferred consultants and attorneys to be involved in the event of a loss because they already know your business operations, it is a good idea to ask to add these professionals to the insurer's pre-approved list during the underwriting process.

Cyber policies also often contain consent provisions stating that the insured must obtain the insurer's consent before incurring any expenses to notify customers or patients of a data breach, conduct forensic investigations or defend against third-party claims. Such prior consent provisions are sometimes invoked by insurers to deny coverage when emergency costs have been incurred without the insurer's consent, even if the costs are entirely reasonable and necessary. If prior consent provisions are included in the policy and cannot simply be removed, you should, at a minimum, change them to provide that the insurer's consent "shall not be unreasonably withheld."

It is also a good idea to keep your insurer on speed dial when a breach happens so that it cannot assert that it has been kept in the dark about any emergency-response costs you incurred.

6. Allocation of Defense Costs

Where both covered and non-covered claims are asserted in the same lawsuit against the insured, an issue often arises regarding the proper allocation of defense costs: what portion of the insured's defense costs must the insurer pay? There are a number of ways that insurance policies can respond in this situation, with some policy provisions being more advantageous to the insured than others.

For example, some policies provide that the insurer will pay 100% of defense costs if the lawsuit alleges any claim that is potentially covered. Others say that the insurer will only pay the portion of defense costs it unilaterally believes to be covered until a different allocation is negotiated, arbitrated or judicially determined.

These issues are less likely to arise in a "duty to defend" policy (where the insurer must assume the insured's defense of any third-party claims), which typically covers 100% of defense costs so long as any of the claims against the insured is potentially "covered." However, under a "duty to reimburse" policy (where the insurer agrees to reimburse the insured for its defense costs or pay them on its behalf), allocation is more likely to be disputed. It is important to understand the allocation method contained in the policy. Try to negotiate one up front that is favorable to you.

7. Obtain Coverage for Vendor Acts and Omissions

Chances are that at least a portion of your organization's data processing and storage is outsourced to a third-party vendor. Therefore, it is crucial that your cyber policy covers claims against you that result from breaches caused by your data management vendors.

Most cyber policies provide coverage for such vicarious liability, but not all do. It is widely understood in the insurance industry that policyholders expect coverage for claims that arise out of the acts and omissions of their vendors, consultants and subcontractors. If such coverage is not initially offered, or is at all ambiguous, you should demand that it is clearly included in the policy.

8. Dovetail Cyber Insurance with Indemnity Agreements

You should also ensure that your cyber policy and vendor indemnity agreements complement each other so you can maximize your recovery from both sources. Some cyber policies state, for example, that the policy's deductible or self-insured retention "shall be borne by the insured [and remain] uninsured at its own risk." Some insurers may interpret this language as requiring the insured to pay the deductible or retention out of its own pocket, and take the position that if the insured gets reimbursed for this amount from the vendor that caused the breach, then it has failed to satisfy this precondition to coverage.

This kind of clause can present you with a Hobson's Choice: either pursue indemnity from your vendor and give up your insurance, or collect from your insurance company and let the responsible vendor off the hook. This unfair outcome is not in the interest of either insurer or insured. As a result, insurers are often willing to modify these provisions to clarify that the insured can collect its self-insured retention from a third party without compromising its insurance coverage.

9. Align Cyber insurance with Other Insurance

Some cyber policies also cover claims made against you for losses caused by data breaches suffered while the data is in your third-party vendor's custody. There may be business reasons for wanting vendors to be insured under your policy in a particular case. But it is generally better to contractually require your vendors to obtain their own cyber insurance to act as the primary coverage for claims, and to also require that they name you as an additional insured under that policy. Then, arrange for your policy to state that it will only apply to claims against you arising out of your vendor's data breach in excess of that vendor's insurance. This structure can reduce the odds that your insurance policy limits will be depleted by claims for which your vendors are primarily responsible.

10. Get a Partial Subrogation Waiver

If your insurer pays a loss, it may become "subrogated" to your claims against any third parties that were responsible for causing the breach. This means that the insurer can try to recoup its payment to you by pursuing your claims against the responsible parties. Many cyber policies contain a provision stating that you cannot take any action to impair the insurer's subrogation rights.

One problem with such provisions in the cyber context is that contracts with data management vendors commonly include limitation of liability provisions. These provisions can give rise to disputes about whether you have breached your insurance contract by impairing or limiting your insurer's recourse against the culpable vendor.

A possible fix is to insist that a partial "waiver of subrogation" provision be added to your cyber policy. Such provisions, which are quite common in other lines of coverage, simply provide that the insurer will not assert that its subrogation rights have been impaired by any contract into which you entered before a loss occurs. Some insurers are willing to agree to such provisions in the cyber context, but others may not be. If your insurer is not willing to give a partial subrogation waiver, you should consider shopping elsewhere.

If you have any questions about the content of this alert, please contact the Pillsbury attorney with whom you regularly work, or the author below.

James P. Bobotek (bio)
Washington, DC
+1.202.663.8930
james.bobotek@pillsburylaw.com

About Pillsbury Winthrop Shaw Pittman LLP
Pillsbury is a full-service law firm with an industry focus on energy & natural resources, financial services including financial institutions, real estate & construction, and technology. Based in the world's major financial, technology and energy centers, Pillsbury counsels clients on global business, regulatory and litigation matters. We work in multidisciplinary teams that allow us to understand our clients' objectives, anticipate trends, and bring a 360-degree perspective to complex business and legal issues—helping clients to take greater advantage of new opportunities, meet and exceed their objectives, and better mitigate risk. This collaborative work style helps produce the results our clients seek.