HUNTON& WILLIAMS

Lawyer Insights

March 1, 2017

# Digital Due Diligence: Four Questions to Evaluate Cyber Insurance Coverage

*by Walter Andrews and Jennifer White*

*Published in Risk Management*

With all the talk of the dangers of hacking and the importance of addressing the wide range of cyberrisks facing every organization, it is understandable that many have reached the point of cyber overload. Cyber and crime insurance policies have been so heavily recommended and purchased that many businesses are ready to move on once policies are placed. But the desire to just be "done with it" can cause a business to cut corners, which risks coverage, or allow unnecessary gaps in coverage, which risks the business. Ignoring the risk, or treating it as something that can be fully resolved, will only increase your company's exposure to potential loss. Therefore, it is important to consider the following four questions to make sure your cyber coverage is meeting your company's needs.

**1. What did we say about our business in the cyber insurance application, or at renewal?**

Cyber applications tend to be lengthy. Insurers want to know about basic demographics like revenue or number of employees, but also often want detailed responses on the amount of confidential information in the insured's possession, data retention policies, privacy policies, computer systems controls, content controls, and prior claims or circumstances. Many applications ask the insured to warrant the conduct of third parties (such as whether the cloud service provider has met all security compliance requirements), or pose "yes or no" questions that may require an explanation instead (such as whether the applicant is in compliance with its privacy policy)

Renewal applications are even more dangerous. Their short length lulls businesses into believing that a lower level of diligence is required for the renewal than was exerted for the original submission. As a result, renewals are frequently signed without reviewing prior applications and without informed responses to the questions asked. Thus, renewals create risk that the signatory will attest to the veracity of a statement about the business or its practices that is no longer true or was subject to a material change.

How a business answers questions in original and renewal applications matters because the policies are placed in reliance on those answers. Indeed, renewal applications incorporate prior application submissions. Applications and policies state that any misrepresentations, omissions, concealments or incorrect statements in the application are grounds for rescission of the policy.

Courts have granted rescission based on even unintentional omissions, or failure to qualify or correct incomplete or inaccurate answers. While not a cyber case, last year in H.J. Heinz Company v. Starr Surplus Lines Ins. Co., the court ordered rescission of an accidental contamination and government recall insurance policy based on what the jury found to be unintentional misrepresentations and omissions about Heinz's claims history.

The risk in the context of cyber insurance is no different. For example, Columbia Casualty Company refused to cover the settlement of a data breach class action based on the claim that its insured, Cottage Health Systems, failed to "continuously implement the procedures and risk controls identified in its application." The disputed answers were to questions like, "Do you re-assess your exposure to information security and privacy threats at least yearly, and enhance your risk controls in response to changes?" and "Whenever you entrust sensitive information to third parties, do you perform due diligence…to ensure that their safeguards for protecting sensitive information meet your standards?"

To avoid the risk of rescission based on application answers, businesses must ensure full disclosure, know what has been submitted as part of their applications, and qualify answers as necessary. Also, key technical personnel should be involved in every application and renewal, and past applications should be reviewed before any renewal is finalized.

**2. Do we have the right "triggers"?**

Your business may have state of the art security, but you can still get hacked. Your business may have unusually high compliance with security and data privacy protocols, but employees slip up. In such instances, you will ask, "Are we covered?" Your policy may not provide the same answer in both scenarios, however, because coverage triggers vary considerably between insurers. For some policies, it is enough that a security incident occurred (answer: coverage for both scenarios). Others will require an extra element of proof, such as whether the insured affirmatively "failed" to do something (answer: possibly no coverage under the first scenario, and coverage under the second). Proof of failure may be difficult if the issue was not your preparedness but rather the skill of your criminal opposition. Thus, you must look carefully at what types of incidents and actions must occur for there to be coverage.

Another "trigger" question is whether the policy applies upon discovery or occurrence of the breach. This is important because cybercriminals are adept at covering their tracks and companies often take considerable time to detect a breach or data incident. Discovery/occurrence triggers can be difficult to negotiate, thus, your business must work with your broker and coverage counsel to build coverage around these triggers to account for their deficits.

The final "trigger" question centers on costs: Does the policy cover costs associated with alleged or suspect breaches? Of course, coverage for events that actually occur is critical, but the cost to investigate and respond to suspected breaches can be nearly as burdensome. For example, your business may hear from a vendor that the vendor has been breached and thinks that your network may have been compromised as well, or maybe a government agency like the FBI says it has found confidential business or personal information from your server somewhere it does not belong. In each of those circumstances, you will incur costs to figure out whether anything happened and, if so, the cause, scope and your subsequent reporting duties. The best coverage applies to the forensic work necessary to do all of those things, which can ultimately help you remedy the situation and patch security vulnerabilities.

**3. What are our gaps in coverage for cyberrisk, and how do other policies or endorsements fix those gaps?**

Cyber policies are improving but will likely continue to lag behind emerging threats. In fact, some policies have not even caught up to existing risks. For example, it is common that policies will cover ransoms paid to prevent the threat of breach, but not ransoms paid to return what has already been taken or remedy the damage that has already been done. Businesses should discuss emerging threats with their broker, and read the policy (with the assistance of the broker or counsel) to determine whether it addresses those threats.

Do not assume that the risk is necessarily covered simply because you have a cyber policy, or because the insurer purports to understand your business and its challenges. The P.F. Chang's case from 2016 illustrates why this is so important: The restaurant giant wanted coverage for payment card industry data security standard (PCI-DSS) assessments, but could not prove that desire was reflected in its cyber insurance policy. This, in part, meant that $2 million in fees and assessments were not covered. Businesses should demand specific policy language for specific risk, especially for exposures like PCI-DSS assessments.

Crime policies may fill some of the holes that cyber policies leave exposed, but even those policies may be insufficient to address creative or complex criminal schemes. The Apache Corporation learned this lesson after wiring $7 million to a fraudulent bank account that appeared to belong to one of its vendors. The scheme was multi-pronged and convincing: It started with a phone call, which the criminals later followed with an email that appeared to use the vendor's letterhead. The letterhead contained a false telephone number, which Apache personnel used to confirm the change request.

Ultimately, the Fifth Circuit Court of Appeals agreed with the insurer's denial of coverage, holding that the loss was not a "direct result" of the email but rather caused by human error in failure to investigate the scheme. A well-crafted endorsement to remove the word "direct" from the computer fraud-insuring clause or a standalone policy to address social engineering may have avoided this outcome.

Also, check your legacy coverage to determine how those coverages address cyberrisk. What exclusions apply, and should any be carved back? And, if you have added cyber-related coverage to any of those forms, does the added coverage actually do what you want it to do?

Last year, in Camp's Grocery, Inc. v. State Farm Fire and Casualty Company, a Piggly Wiggly franchisee learned the hard way that an "electronic data" coverage extension did not provide the breadth of coverage it needed to address its risks. The grocer was sued by credit unions after cardholder accounts were stolen from the grocer's computer network. The losses included, among other things, the costs to reissue the cards, reimburse customers for fraudulent charges, and the value of diminished goodwill. Camp's sought coverage from its business insurer, specifically under its inland marine computer property form, which covered "accidental direct loss" to "electronic data," including some types of customer data. The court held that the form only provided first-party coverage for loss to Camp's, however, not third-party coverage for the credit unions' suit. The case is a good reminder that a business cannot treat cyberrisk protection as it would a coin toss; instead, a business must cover its head and its tail.

To ensure this type of comprehensive protection, it is good practice to review policies for gaps each year, even after well-crafted and broad forms are in place. New technologies, new threats and new business activities mean that even the best policies may need to be tweaked. When reviewing, keep in mind your business's claims history, including events that would not be large enough to trigger coverage or constitute a claim. Assume losses from those events had been worse, and then check to see if your policy covers the risks.

**4. Do we have the right advocates?**

The best coverage depends on the best advice of your broker and coverage counsel. Their advice is particularly important in the cyber insurance realm because the policies are relatively untested in court and vary widely between insurers.

Your broker and coverage counsel should both express the desire to learn about your business and then actually do so with your assistance. An understanding of the market (for your broker) or the law (for your attorney) is important, but, by themselves, will not ensure that your business obtains the right coverage for your risks. Talk to them about what you do, how you are structured, and the concerns of your critical leadership, including human resources, information technology and marketing. Even "simple" businesses are complex, and detailed conversations uncover nuance about procedures, practices and employee roles that are not immediately apparent. The gaps in coverage usually hide in the nuance.

Your broker in particular needs to be a good advocate for your business. This means he or she should know the market, understand how coverages differ, and know how and when to push for revisions by endorsement. This also means that you should understand the brokerage firm's market power, how it assists clients in similar industries, and the nature of its relationships with insurers.

Your coverage counsel should work with your broker to draft the best coverage language possible, as both add value to the cyber insurance placement process. Experienced coverage counsel can analyze policy language through the lens of potential litigation, advising the insured about coverage issues based on identified risks, and giving brokers the ammunition they need to negotiate endorsements. Indeed, coverage counsel sometimes may be more effective at negotiating changes, especially when insurers claim to be unwilling to revise policy language. Either way, counsel should help solve your coverage problems, not be an additional impediment to coverage.

Finally, when you find people you trust, make sure you can use them when the time comes. Most policies allow the insurer to select breach response providers—usually from a list of pre-selected attorneys and vendors. Often, insurers are willing to approve additional firms and vendors that you would prefer to use instead, especially when those entities know your business or have unique, industry-specific expertise. It is well worth it to ask, given the relief that comes from working with a "known entity" when responding to the many "unknowns" of a security breach.

Walter J. Andrews is a partner in the Miami office and head of the insurance litigation and recovery practice at Hunton & Williams LLP. His practice focuses on complex insurance litigation, counseling and reinsurance arbitrations and expert witness testimony. Walter can be reached at (202)955-1802 or WAndrews@hunton.com. Jennifer E. White is an associate in the Washington, DC office. Her practice focuses on insurance coverage counseling and litigation, with an emphasis on cyber insurance matters. Jennifer can be reached at (202)955-1866 or jewhite@hunton.com.