Does Your Law Firm Have Insurance Coverage for Cyber-Related Risks?

Patrick M. McDermott and Sergio F. Oehninger

Patrick M. McDermott is an associate with Hunton & Williams in Washington, D.C. He may be reached at pmcdermott@hunton.com. Sergio F. Oehninger is of counsel to Hunton & Williams in Washington, D.C. He may be reached at soehninger@hunton.com.

Not a week goes by without news of a new cyber attack. Law firms are not immune. In the ABA 2015 Legal Technology Survey Report, 15 percent of respondents disclosed that their law firms had a prior security breach. And the victims of these breaches were not limited to large firms. Indeed, about 10 percent of solo practitioners and 15 percent of firms with fewer than 10 attorneys reported previous breaches.

As one example, in early 2015, a four-attorney firm in California was subjected to a "Cryptolocker" cyber attack. There, the hackers likely obtained access to the law firm's servers with a phishing email, which usually includes a link that, if clicked on, will install malicious software on the computer. Then the software encrypted the law firm's files and the hackers threatened to destroy the files unless the firm paid a ransom. The firm reported that it did not pay the ransom but said that the attack resulted in only a minor loss of data due to backups and hard copies of documents. Had the malware infected the backup data or downloaded the data, the impact to the firm could have been much more severe and costly. Insurance is one way that firms can help minimize the losses resulting from such attacks.

However, firms should not rely solely on their ability to obtain coverage for cyber attacks under typical liability policies. Court decisions evaluating their applicability show why. For example, coverage for data breaches under general liability policies can depend on whether there is "publication" of private information. A federal appellate court recently found publication of private medical records where those records were accessible on the Internet through a simple Google search without showing that any third party accessed them. On the other hand, a New York state court found no publication and thus no coverage where a third-party hacker and not the policyholder had published the information. Another relevant question that can arise under general liability policies is whether the loss of electronic data is "physical loss or damage"; court decisions go both ways on this issue as well. Similarly, policies that insure against legal malpractice claims may not cover claims arising out of cyber-related events even though attorneys' obligations to their clients are affected by such events (for example, maintaining confidential information).

To better protect against losses resulting from cyber attacks, firms should consider purchasing coverage specifically written to cover cyber-related losses. That coverage is now available on the market. For instance, Florida Lawyers Mutual Insurance Company, an insurer offering professional liability insurance to Florida lawyers and created by the Florida Bar, offers cyber liability coverage for law firms. USI Affinity, which offers coverage to lawyers in New York, can similarly provide cyber liability coverage to firms.

Applications for cyber coverage can be particularly time-consuming, not least because of their technical nature. Firms should take the time needed to provide accurate answers rather than later face an insurer's claim that an allegedly inaccurate response on the application avoids coverage.

Firms should also consider their potential losses to help identify the areas in which cyber coverage is needed. Possible losses include those related to business losses, including lost income, reputation, and digital assets; repair, including restoring or replacing data; ransom; notifying clients and related credit and identity monitoring; forensic analyses undertaken post-breach; public relations efforts; legal fees; and statutory and regulatory fines or penalties.

Because of the wide-ranging nature of potential losses and the differences in coverage provided by cyber-related policies, price alone should often not be the determining factor in choosing a policy. The cheapest policy may also provide drastically less coverage than a pricier one. Among other things, firms should carefully consider what losses the policies covers, including whether there is coverage for data loss, physical loss, business loss, and losses related to responding to data breach. Different coverages in cyber policies are often subject to various limits, sub-limits, deductibles, and retentions, so firms should also evaluate those items.

After purchasing cyber coverage, a firm should maintain the policy in an easily accessible location. This includes maintaining a hard copy of the policy because you may need it most when your electronic files and computers are unavailable. If your firm is subject to a data breach or other cyber incident, identify all potentially applicable policies—whether cyber-specific or not—and comply with the notice requirements in those policies.

Cyber policies may contain requirements that the policyholder identify specific coverages or sublimits within the policies and may also require the policyholder to select third-party vendors in order to obtain coverage for expenses related to investigating and resolving cyber attacks. So, while firms should take care in reviewing all potentially applicable policies, they should take particular care in reviewing the potentially applicable cyber policies. In addition to the benefits of avoiding insurer claims that notice was provided late, giving an insurer notice of a cyber incident early can prove helpful as the insurer may have more experience than the policyholder in dealing with cyber incidents.

Cyber attacks are a real threat to all businesses, including law firms of all sizes. Cyber attacks and other cyber-related events can be costly, even catastrophic. Firms should therefore carefully consider their options for insuring against such events, including by purchasing insurance coverage that specifically covers cyber-related losses.