Misperceptions about Insurance May Leave Law Firms Vulnerable to Financial Consequences of Cyber Attacks

By Eileen Garczynski

Despite the proliferation of specialized insurance policies to address Internet and cyber exposures, many law firms still mistakenly believe they have adequate protection under cyber-related coverage extensions to their existing professional liability insurance. At the same time, they lack familiarity with the nuances of stand-alone cyber-liability insurance policies, which may leave them with serious gaps in their coverage.

In particular, there is a misperception among firms that adding a network endorsement to their lawyers' professional liability policy will address most of the cyber-related exposures they face. Unfortunately, that isn't the case. In fact, the endorsement typically covers only the costs to repair a firm's computer system that sustains damage from a cyber attack. While those costs can be significant, especially for larger firms, the endorsement leaves firms completely uninsured for potentially more substantial costs associated with lost billable time, regulatory fines, or credit monitoring.

This is a fundamental reason for law firms to evaluate stand-alone cyber-liability insurance policies—and do so with the understanding that these insurance policies are not all equal. They also should recognize that insurance coverage altogether is not a panacea for addressing the full spectrum of a law firm's cyber-related exposures. For law firms of all sizes, the effective management of cyber exposures requires a comprehensive approach that includes a thorough risk assessment, educating employees and vendors, strengthening security measures, establishing an incident response plan, as well as the careful evaluation and purchase of appropriate insurance coverage.

NEED TO SAFEGUARD CONFIDENTIAL INFORMATION

Most law firms handle substantial volumes of confidential client data. That includes information about the clients' business practices, intellectual property, trade secrets, pending business transactions, and legal strategy. Firms also may have significant employee and client health data and information protected under the Health Insurance Portability and Accountability Act (HIPAA).

However, coverage under most cyber-liability insurance policies may be limited to claims resulting from the theft or inadvertent disclosure of personally identifiable information, such as social security numbers, driver's license number, birth date, etc. So, it's critical for law firms to obtain a cyber policy that defines "confidential information" more broadly to include all materials that fall under the attorney-client privilege.

As with numerous cyber attacks that occurred in the past several years, these incidents often can result in negative media coverage for victimized firms and involve substantial costs. In addition, if the law firm's information technology system is incapacitated or inaccessible for any amount of time, the firm may lose significant billable time.

Eileen Garczynski *is a senior vice president and partner at Ames & Gough. She also is a member of the American Bar Association's Standing Committee on Professional Liability. Portions of this article were adapted from the American Bar Association guide, "Protecting Against Cyber Threats: A Lawyer's Guide to Choosing a Cyber-Liability Insurance Policy," by Eileen Garczynski.*

A cyber attack also will involve the cost of forensic investigations to identify the cause and spot system vulnerabilities, as well as potential federal and state regulatory fines and notification costs. Other fallout from these incidents includes issues with third parties; lawsuits, reputational damage, and disgruntled clients.

For law firms, in particular, there's the specter of potential ethical issues. Inadequate data security or protection of privacy might be considered a failure to abide by the duty of confidentiality.

Under Rule 1.6 of the ABA Model Rules of Professional Conduct, "a lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent." The rule stipulates that attorneys must "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."

MANY ELEMENTS TO MANAGE CYBER RISK

Although they have become targeted in a growing number of cyber attacks, law firms still trail several other professions and many industry sectors when it comes to measures taken for data protection. With that in mind, here are some of the basic elements law firms should have in place to assess and manage their potential vulnerabilities to cyber attacks.

CONDUCT A THOROUGH RISK ASSESSMENT

Law firms should thoroughly inventory all confidential data owned or maintained by the firm and check to make sure that appropriate data management protocols and security procedures are in place for safeguarding all information.

In addition to conducting frequent risk assessments, firms should invest in state-of-the-art security measures. It also is prudent for firms to consider hiring "ethical hackers" to test data security.

Here's something to keep in mind: A firm's size or visibility isn't necessarily the biggest factor in whether or not it is targeted by cyber-criminals for an attack. In fact, most firms are targeted because of exploitable security weaknesses. As a result, it makes sense to test integrity of the law firm's information management system on a regular basis.

EDUCATE EMPLOYEES AND VENDORS ALIKE

Law firms should make sure they have adequate processes and communications measures in place to inform employees about their role in securing information of the firm and its clients.

In addition, all vendors should be informed of appropriate security procedures and understand their role in the process. These measures should be reviewed periodically as well as whenever data security policies are updated.

FOCUS ON PREVENTION

There are several actions law firms can take to help prevent breaches from occurring. These include:

- **Requiring passwords.** Firms should require the use of effective passwords by all employees. Passwords should be at least 12 characters, and changed regularly.
- **Encrypting hardware and media.** Laptops should be protected with whole-disk encryption without exception. In addition, all backup media and thumb drives should be encrypted and activity on all USB ports should be logged.
- **Establishing equipment standards.** Firms might consider providing a standardized desktop with firm-issued-only software.
- **Securing servers and all hardware.** All firms are vulnerable not only from cyber-attacks launched over the Internet, but also from physical theft of their hardware. While safeguards should be established for all devices, including laptops, mobile phones and tablets, the firm's servers should be secured in a locked rack in a locked closet or room.
- **Setting protocols for software procurement and maintenance.** Solos and small firms should use a single integrated software product to deal with spam and viruses and patches should be applied on a timely basis to any software products found to have potential vulnerabilities.

- **Employee termination security protocols.** When terminating an employee, firms should be sure to cut all possible access (including remote access) to the network immediately and cancel the employee's ID.
- **Establishing protocols for all remote access.** Law firms should weigh carefully the benefits and risks of providing employees system access from home computers or laptops. Employees also should be required to follow the firm's guidelines for accessing wireless hotspots. For all remote access, employees should be required to use a virtual private network (VPN) or other encrypted connection.

CYBER INCIDENT RESPONSE REQUIRES SOUND PLANNING

Law firms should approach the potential for a security breach not in terms of "if" something were to occur, but rather "when" it will occur. An effective response requires being proactive and investing the time to develop a sound plan.

An important first step involves creating a response team to develop and implement a plan of action when a breach or other cyber event occurs. The team should be multi-disciplinary and the plan should include procedures for promptly identifying and repairing the breach, investigating the cause, analyzing the implications, and notifying all necessary parties including clients, vendors and any affected employees or other individuals in compliance with any federal or state disclosure requirements.

REVIEWING INSURANCE AND PROCURING APPROPRIATE COVERAGE

Cyber-liability insurance should be considered a critical component of every law firm's risk management portfolio along with a comprehensive incident or breach response plan.

In evaluating their cyber-liability insurance coverage options, law firms should make sure any policy they procure provides primary coverage, which means it will respond immediately in the event of a data breach or other incident. A high percentage of cyber-liability insurance policies state that they are "excess" over any other insurance.

That means a law firm would have to exhaust any applicable coverage available under its other insurance policies, such as professional liability insurance, in order to access the proceeds of the cyber-liability policy. Indeed, law firms will not want to have their professional liability insurance used for cyber risks when it should be expressly to address malpractice claims.

Before choosing a cyber-liability insurance policy, carefully consider the scope of coverage and exclusions under a data breach policy, including whether the policy covers costs related to lawsuits, regulatory investigations, internal investigations, notifications to affected consumers, public relations management, credit monitoring, and/or statutory penalties.

Stand-alone cyber-liability insurance policies, which can address both first- and third-party perils, offer a full range of protection for mitigating risk. The policies typically provide coverage through a combination of several different insuring clauses that afford coverage for losses arising out of data or privacy breaches. These include expenses related to the management of an incident, such as forensic investigation, remediation, notification and credit checking.

Cyber-liability insurance policies also can provide some coverage for business interruption losses, extortion network damage, and regulatory investigation costs arising out of a cyber event.

The first-party coverages, especially business interruption, can be particularly valuable for law firms whose systems go down as a result of a cyber attack—even for just a few days. In these cases, firms may lose significant amounts of billable time. However, a well-structured cyber-liability policy can cover lost billable time by averaging the last three months of billables and calculating the cyber-related loss on that basis.

SMART SHOPPING: WATCHING FOR CYBER LIABILITY COVERAGE RESTRICTIONS, EXCLUSIONS AND LIMITATIONS

Even though cyber-liability insurance policies have developed over time and offer many coverage features that enable buyers to address this exposure, there's a wide disparity in how these policies are worded, which ultimately affects the amount of protection they provide and how and whether they will respond in the event of a claim.

So, buyers beware: Pay careful attention to specific coverage clauses and exclusionary language. Be sure to understand exactly what the insurance covers, the extent of coverage provided, and any specific coverage exclusions or restrictions. Indeed, many insurers will attempt to add exclusions either through the policy wording itself or by endorsement. Law firms need to be aware of them, understand how they might affect their coverage, and make an effort in collaboration with their insurance advisors to attempt to get them removed or revised to be less restrictive.

In addition to how they define "confidential information" (as mentioned earlier), today's cyber-liability policies contain as many as a dozen or more coverage exclusions or restrictions, including the following:

- **Encryption exclusions.** Certain cyber-liability insurance policies exclude coverage if the firm's mobile devices are not encrypted. As stated, encrypting these devices is sound risk management; however, coverage should be provided regardless of whether or not this is done.
- **Retroactive date.** This is an increasingly complicated issue in light of the fact that a number of breaches occur when a system is actually infiltrated several months or longer before an attack is ultimately detected. Some cyber-liability policies exclude coverage for a specific retroactive date or for claims the firm could have reasonably foreseen. For practical purposes, firms should limit knowledge of claims to key individuals within the firm. In terms of their insurance policy, it's worth noting that under the better cyber insurance policies coverage is triggered by the "discovery of the network security event" and not the occurrence of the incident. In such cases, there's no need for full prior acts or a retroactive date prior to the policy's inception.
- **Definition of damages/loss.** Certain risks covered by cyber-policies may have unique remedies and involve related costs. For example, privacy violations can result in a duty to notify affected individuals and to provide credit monitoring for defined periods of time following the violation. Law firms should be sure the "loss" as defined and covered by the policy addresses the types of relief they may be required to provide.
- **Data outside an insured's network or premises.** This policy wording should be reviewed carefully and particularly is relevant for any firms using cloud providers and other outsourced vendors. Today, most cyber-insurance policies define a "computer system" to include third-party networks with which the firm has contracted for support services. Thus, in the event of a breach, the policy will respond regardless of where data were stored when the breach occurred. Thus, the coverage should apply to the data, irrespective of where they are stored.
- **Voluntary notification of a breach.** Most states and various countries have enacted breach notification laws. Generally, they require firms that lose sensitive personal data to provide written notification to all individuals potentially affected. Even when not required by law, many firms now provide such notification as a matter of prudent business practice. However, not all cyber-policies cover costs of providing a breach notice; check whether and how the policy will respond to these circumstances.
- **Restrictions on investigative, defense and settlement costs for issues related to civil penalties and fines.** While most cyber-liability policies cover civil fines or penalties imposed by a government agency, and costs incurred in connection with a government investigation, some limit coverage to what's insurable by law in the relevant jurisdiction. This raises legal questions not specified in the policy terms; policyholders may wish to consult with their corporate risk and legal departments, as well as with their other professional and legal advisors.

In addition to these policy coverage issues, there are a number of other policy restrictions to consider carefully. For example, in a number of cases breaches have been caused by disgruntled employees. All types of commercial insurance policies contain a specific "conduct exclusion"; with respect to cyber-liability policies, law firms should make sure this exclusion is strictly limited to dishonest, fraudulent, or criminal acts committed by the firm and/or its senior management.

While most data and security breaches result from negligence, such as an ineffective firewall, many breaches are caused by malicious acts, perpetrated or assisted by insiders. Law firms should seek an exception to the conduct exclusion for "rogue" or disgruntled employees to guarantee coverage for malicious conduct by individuals inside the firm.

Law firms also should note that the conduct exclusion for fraudulent or criminal acts of senior management should be worded to apply **only after final adjudication**, or determination, that the excluded conduct did, in fact, occur.

Another potential coverage issue law firms should note has to do with theft of hardware. Many cyber-liability insurance policies don't cover theft of hardware from the insured's premises and limit protection for breaches to those involving only US privacy statutes or regulations.

COVERAGE SHORTFALLS

Many policies have inadequate sub-limits for forensics and crisis management expenses, which can leave law firms without sufficient funds to investigate where their systems were infiltrated or to address the costs of effectively managing a related crisis event. Cyber-liability policies also contain restrictions for restoration of intellectual property or proprietary business information. When related coverage is provided, it typically is limited to amortized value.

Another area to check involves the policy's requirements for using vendors to address data breaches and related issues. Many insurers require policyholders to use their designated preferred vendors; changing this language to allow a law firm to choose its own vendors may require an additional premium.

POLICY WAITING PERIODS

Cyber-liability insurance policies typically have an aggregate limit of liability (or the total dollar amount available to pay claims incurred during the policy period), as well as specific sub-limits that apply to each first-party coverage and the fines and penalties related to third-party coverage.

The good news for law firms is that the sub-limits generally have increased in recent years, so insured firms can typically get up to 50 percent of the total limit to apply to first-party costs. A dollar deductible also applies to each of the coverages provided that varies by policy size and firm insured. Beside the dollar deductible, most policies include a "time element" or waiting period deductible to trigger the first-party business interruption coverage.

For example, a cyber policy might require the network to be down for more than 12 to 24 hours before the business interruption coverage would apply. Law firms should be aware of these policy features and requirements for reporting incidents and related business loss.

KEYS TO ASSESSING COVERAGE REQUIREMENTS

A key challenge for many law firms involves determining how much cyber-liability insurance they need. For many, the starting point in this analysis goes back to the overall assessment of their potential risk.

Firms that maintain large amounts of personal identifiable information, intellectual property, or highly confidential information either for clients or staff, may require higher limits.

Another consideration in evaluating appropriate limits, involves estimating the firm's first-party costs when a cyber-breach occurs. These costs include lost billing time, forensic investigation, legal fees to determine regulatory or notification obligations, notification, communication, and public relations costs, credit monitoring, and regulatory fines and penalties.

Third-party costs also may be significant. They include settlement/damages to third parties, legal fees to respond to a third-party loss, damages to network security of a trading partner or vendor, intellectual property infringement, and regulatory proceedings.

Following an analysis of potential costs associated with a cyber breach, the firm should determine the amount of risk it chooses to retain. This can be either by not purchasing insurance at all or through a deductible or retention.

Keep in mind that even law firms with well-established safeguards to prevent cyber attacks, still face these risks. It's worth noting that recovery costs from such incidents can be substantial. In determining insurance needs, it's prudent to consider the worst-case scenario.

Finally, firms need to consider their contractual obligations to have cyber-liability insurance. For instance, firms with institutional clients may be contractually required to purchase minimum limits of cyber-liability insurance. Increasing numbers of law firm clients, particularly financial institutions and health groups, for example, are requiring their counsel to carry this insurance.

In the face of increasingly challenging exposures related to Internet and cyber attacks, law firms need to mount a comprehensive effort to manage these risks. Besides recognizing the limitations of protection available under their existing insurance policies, such as professional liability, law firms should carefully evaluate the purchase of standalone cyber-liability insurance. In assessing these policies, they should review coverage exclusions, restrictions and limitations, and work with experienced insurance advisors to remove or revise restrictive wording. At the same time, implementing sound risk management remains a key element along with insurance to their overall protection from expanding cyber threats.