

THE RECORDER

Insuring Against Cyber Crime

W. Brian Ahern and Christine Clark

February 09, 2011



Brian Ahern, Ahern Insurance Brokerage
Image: courtesy photo

Cyber liability is increasingly important for law firms and lawyers. Technology has created new issues concerning breaches of privacy, security and more that can severely affect a law practice. Approximately 10 million victims a year are affected by a breach of privacy. Forty-six states have enacted data breach notification legislation, and federal law includes host data security requirements. Stolen laptops or other data-bearing devices rank the highest in terms of risk and provide access to your technology systems and confidential information.

A breach can be costly. Lost billable time can be extensive. Costs to restore damaged/destroyed data can be exorbitant. It takes approximately 175 hours to resolve the issue when a breach occurs. With the estimated cost to rebuild records at \$202 per record, law firms can accrue significant fees.

While the risks are great, insurance litigators are in agreement that law firms have been "slow" to purchase cyber insurance. Many firms assume coverage will be offered by their directors and officers, errors and omissions, or commercial liability policies. However, in many cases, such coverage is not adequate. After examining their existing policies and applicable exclusions, many law firms find that there are a number of potential fact patterns and claim scenarios typically not covered by existing policies, including computer hacking, lost laptops and backup tapes, stolen computer equipment, transmission of a computer virus, state and federal fines (e.g., HIPAA and new red flag rules), and costs associated with state privacy notification laws.

Insurance experts also note that many law firms assume that a breach won't happen to them. However, law firms are ranked ninth in terms of organizations with the highest risk of cyber exposure. Every day, the number of cyber attacks grows. While news accounts may feature big corporations that have been hacked, smaller companies are also victims.

Law firms often believe that if they are victims of a cyber breach, they can absorb the cost/be self insured. The costs can be substantial and cover a range of unexpected areas. Consider the following losses that could arise out of a single incident:

First party — direct losses incurred by a law firm such as data recovery or business interruption expenses.

Third party — damages, civil fines or penalties, and claims from third parties (such as clients) and/or regulatory authorities.

Network security — damages and claims expenses arising out of computer attacks caused by a security failure, including theft of client information, identity theft, negligent transmission of computer viruses and denial of service liability.

Internet/media liability — claims resulting from information on a website or through the Internet, such as copyright/trademark, libel, slander, defamation and advertising injury.

Cyber extortion — responding to a demand, including some forms of payment.

Computer crime — damages directly caused by fraudulent input, fraudulent destruction or fraudulent modification of data.

Crisis management expenses — hiring a public relations firm and other professionals to deal with negative aftermath.

The type of law a firm practices is a factor when considering cyber liability exposure. A law firm representing a pharmaceutical company or physicians may have a great deal of personal health information it needs to protect. Names, Social Security numbers, credit scores and bank accounts — all of this personal information is under increasing siege by computer hackers and identity thieves. A single loss of sensitive data, whether through thievery, technical malfunction or sloppy record keeping, not only can damage a firm's reputation, but also expose it to crippling lawsuits.

The average premium for coverage that will protect a firm from cyber liability for \$1 million in coverage with a \$5,000 deductible is approximately \$1,000 annually. As there are several different types of protection, it is important to know the various policy options.

- Privacy: This type of coverage applies to the unauthorized acquisition, access, use, physical taking, identity theft, mysterious disappearance, release, distribution or disclosures of personal and corporate information. Breaches by rogue employees and unauthorized third parties are also covered, as are civil fines and penalties and consumer redress. One of the benefits of this type of coverage is the broad definition of personal information, including third party confidential business information.

- **Technology security:** Despite the best prevention efforts, attacks happened. This type of policy covers the failure to prevent a party from unauthorized access to, use of or tampering with technology, including denial of service attacks. Malicious code or malware (software designed to infiltrate a computer system without the owner's informed consent) coverage is offered through these types of policies.
- **Web-media services:** Personal injury claims can arise from your Internet and intranet website, including the gathering, publication or dissemination of web-based content. Intellectual property issues can arise for any outward or inward facing website your firm maintains. Web-media services coverage provides protection from such claims.
- **Privacy breach containment coverage (including employee records):** If your firm is hit with a breach, under this type of policy the costs of notification and investigation of the attack are covered, as are crisis management expenses and credit monitoring costs.

Technology extortion: Extortion payments to a third party related to a technology threat are covered under this type of policy. Also covered are the expenses to investigate the cause of the extortion and the expenses the law firm incurs to pay the extortion.

- **Data restoration —** Costs to restore, recover or replicate data that is damaged by a technology breach are covered, as are the costs to determine the ability to recollect data and to recollect unrecoverable data.

Your insurance broker can help you review the various types of policies and help decide which coverage you need based upon several factors, including any existing coverage you may have under current policies and your level of vulnerability given the areas of law your practice. With the risks high and the cost of coverage relatively low, no law firm should go without cyber liability coverage.

W. Brian Ahern is president and CEO and Christine Clark is vice-president of Ahern Insurance Brokerage, one of the largest independently owned insurance brokerage firms specializing in the insurance needs of law firms.

In Practice articles inform readers on developments in substantive law, practice issues or law firm management. Contact Vitaly Gashpar with submissions or questions at vgashpar@alm.com.

"Reprinted with permission from the February 9, 2011 issue of The Recorder. © 2011 ALM Media Properties, LLC. Further duplication without permission is prohibited. All rights reserved."