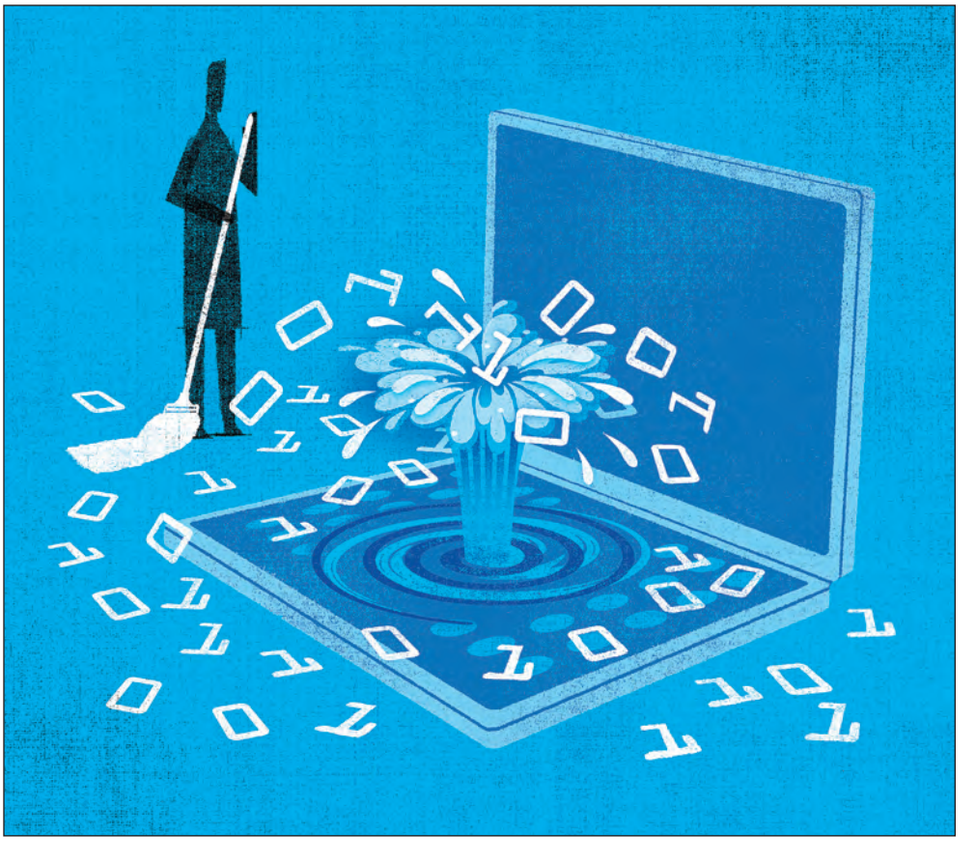
EDITED BY
JAMES PODGERS,
MOLLY McDONOUGH

Practice



Net Risk

Cyber liability insurance is an increasingly popular, almost necessary choice for law firms by David L. Hudson Jr.

Ethics

It is no secret that law firms handle loads of sensitive, private data of clients, third parties and others in the course of conducting business. Unfortunately, there are many ways that health information, Social Security numbers, credit card numbers and other personally identifiable information can be compromised —whether by a lost laptop, cellphone or iPad; a coordinated insidious attack by hackers; simple human error; a rogue employee; or other causes.

The need for data security applies to many different types of law firms and areas of practice. "For example, a personal injury firm may take credit card payments from clients," explains Anthony Dagostino, vice president of professional risk at the insurer ACE Group. "That credit card information needs to be protected. Practices focused on corporate restructuring or other corporate work focused on an upcoming IPO or acquisition may have confidential corporate information of those clients protected under a nondisclosure agreement or similar contract. Furthermore, a firm handling personal injury suits or medical-malpractice cases could have personal health information in their custody."

The loss of such data can have many negative repercussions, including lawsuits, regulatory investigations, fines and penalties, and the loss of a good reputation as a trusted fiduciary of client confidentiality. For this reason, more and more law firms are following in the footsteps of other industries and purchasing or considering the purchase of cyber liability insurance.

"Law firms today are responsible for

ILLUSTRATION BY JIM FRAZIER

massive amounts of electronic and nonelectronic information," says Chris Andrews, vice president of professional liability at AIG. "Depending on a firm's areas of practice, this information can range from personally identifiable information to protected health information to confidential corporate information, such as intellectual property, contracts, and details on mergers and acquisitions. This information represents significant liability exposure in the event of a security failure. Even if the failure doesn't lead to an actual lawsuit, a firm may still need to deal with costs associated with notification, possible regulatory investigations, fines and penalties, forensic expenses, public relations expenses and more."

Andrews adds that "it's not just third-party information at risk. We've seen instances where the firm's own proprietary information was completely wiped out, leading to costly data restoration and re-creation expenses. We're definitely witnessing a growing appreciation of this risk within the legal industry."

James Brown, chair of the ABA's Standing Committee on Lawyers' Professional Liability, says coverage can help cover costly breaches.

"I certainly do believe lawyers need to ensure they have coverage for cyber liability and, in particular, the costs, which can be substantial, in remedying a breach," says Brown, a shareholder at Liskow & Lewis in New Orleans.

Cyber risk policies were introduced in the 1990s but have experienced a dramatic growth in recent years, according to Washington, D.C.-based attorney Thomas H. Bentz Jr., head of Holland & Knight's team on directors and officers and management liability insurance. "Corporate America has seen a huge increase in the purchase of cyber policies in the last three to five years. Law firms have been slower to follow," Bentz says. "In my experience, it is still not common for law firms to purchase cyber liability coverage. I expect that this will change in the next several years as the potential exposure becomes clearer and the coverage more certain."

"We've seen a noticeable increase in the number of firms who have purchased separate cyber policies over the past 24 months," says AIG's Andrews. "We're probably not yet at the point where we can say it's a common purchase, but it's certainly trending in that direction. Many firms are consulting their clients on privacy and regulatory issues, and at the same time those clients are now asking questions as to how firms use, store and protect information. Given this heightened level of awareness, it makes sense that firms are now looking inward to make sure their own house is in order and cyber coverage is part of the solution."

A key question for a law firm is what data breaches or other cyber risks may or may not be covered by their standard lawyers' professional liability policy. A standard LPL policy may not cover many data breaches.

Dagostino says, "A key question for law firms is whether their LPL has affirmative coverage grants for loss of client or third-party data as well as the out-of-pocket costs associated with responding to the incident."

'NO SILVER BULLET'

Andrews recommends that law firms seriously consider purchasing such policies. "Cyber coverage provides an extra layer of protection, which helps firms mitigate the impact of security failures," he says. "There is no silver bullet, so firms need to be dynamic in their approach to cyber risk—meaning sound cyber risk management should encompass people, policies, procedures, technology and insurance solutions as well.

"Additionally," Andrews notes, "some carriers go beyond just offering an insurance policy and also offer risk management services which firms can use to further protect against these exposures. These services can actually be quite robust and innovative. Finally, insureds are able to tap into a built-in network of IT experts, PR firms and legal counsel experienced in cyber matters, which brings an enormous amount of value to the coverage."

Most carriers "offer a menu of coverages which can be selected depending upon an insured's specific needs," Andrews says. "Coverage generally falls into two categories: third party, which protects against legal liability arising out of security failures and often extends to fines and penalties arising from regulatory actions; and first party, which addresses costs and expenses the insured incurs because of a security failure. This includes costs to mitigate the failure, such as notification and credit monitoring, costs to investigate the failure, such as forensic expenses, and even lost income caused by an interruption of the insured's operations caused by a network security failure."

Experts say that cyber policies often offer benefits and other services not available in a standard LPL policy. "We recommend that law firms look closely at their LPL policy with a fine-tooth comb and identify exactly what coverage and services are provided under the policy," Dagostino says.

"Cyber policies offer 'breach coaches' and other benefits that are likely not available in an LPL policy," Bentz says. Experts posit that many cyber liability policies offer pre-breach and post-breach services that likely are not covered by many LPL policies. "A key pre-breach service relates to security awareness and cyber-readiness. A key post-breach service includes mitigating harm and having a forensic investigator help the firm."

Perhaps the biggest reason for a law firm to at least consider purchasing such a cyber policy is the reality of more exposure. "Law firms are experiencing breaches with increasing frequency and in many different forms," Andrews says. "We expect the number of lawsuits to rise over the next several years." ■

ILLUSTRATION BY JIM FRAZIER