LAW FIRMS CAN TAKE STEPS TO MANAGE EXPANDING CYBER THREATS

by

Eileen Garczynski
Senior Vice President and Partner
Ames & Gough

As hackers and organized crime rings look for new ways to steal funds and gain illegal access to confidential corporate and personal financial information, law firms increasingly have become targets for their actions. Along with personal and confidential health and financial data on employees and clients, many law firms maintain sensitive information on client strategies, trade secrets, and pending business transactions.

A privacy or security incident can involve substantial costs. If a law firm's system goes down for any amount of time, significant billable time may be lost. There's also the cost of forensic investigations to determine the cause of the breach, potential federal and state regulatory fines and notification costs. And when an incident results in damage to third parties, the outcome may include lawsuits, regulatory fines, negative publicity, and disgruntled clients.

Law firms face another damaging consequence of data breaches and information security lapses: potential ethics complaints. Inadequate data security or protection of privacy can constitute 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." Lawyers must "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."

While the multiplicity of technology- and internet-related risks is significant, law firms can take several steps to anticipate, prevent, and respond to a data breach, including the purchase of a cyber-liability insurance policy.

Effective cyber risk management starts with safeguarding data. Catalog all confidential data owned or maintained by the firm and make sure proper security procedures are in place to keep it safe. That includes conducting ongoing risk assessments, investing in state-of-the-art security, and regularly testing the integrity of systems.

Employees and vendors should be informed of security procedures and these policies should be updated periodically and reviewed with them.

Preventing breaches calls for several measures, including: having strong passwords (at least 12 characters) and changing them regularly; protecting laptops, backup media and thumb drives with whole-disk encryption. Firms might also consider a standardized desktop equipped only with firm-issued

software. Servers should be secured in a locked rack in a locked closet or room. Solo and small firms should use a single integrated product to address spam and viruses and make sure software patches are applied on timely basis.

When terminating employees, immediately cut all access (including remote) to the network and cancel the employee ID. Instruct employees to use wireless hotspots with great care and provide a virtual private network (VPN) or other encrypted connection for remote access.

Be prepared. Establish a multi-disciplinary team to develop a plan and respond when a breach occurs. The plan should have procedures for identifying and repairing the breach, investigating its cause, analyzing its implications, and notifying the necessary parties, including the insurance company.

These measures can be complemented by effective insurance coverage. As pricing of cyber-liability insurance has become more affordable, many law firms now view it as a critical element of their overall risk management program. Nonetheless, all cyber-insurance policies are not the same.

It's important to check the scope of coverage provided along with any restrictions or exclusions. In particular, consider the presence and extent of coverage for 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, generally offer a full range of coverage that is key to mitigating this risk. The policies typically have various insuring clauses to address losses arising from data or privacy breaches, such as expenses associated with managing an incident, including those for forensic investigation, remediation, notification and credit checking. They also provide coverage for business interruption losses, extortion network damage, and regulatory investigation costs arising out of a cyber-event.

Evaluate insurance protection. Work with a specialized insurance broker who can advise you on which cyber-insurance policy best meets your firm's needs. Be aware that some of these policies have exclusions that are too broad and can create gaps in coverage.

Law firms should understand their potential impact and, when possible, attempt to have them modified or removed. There are more than a dozen specific types of coverage exclusions or restrictions that might appear in many or some cyber-liability insurance policies for law firms.

For instance, consider how policies define confidential information. Some limit this definition to Personal Identifiable Information (or PII, such as date of birth, Social Security number, driver's license ID, etc.). However, a better policy for a law firm will have a broader definition that includes anything protected under the attorney-client privilege.

During the past several years, most states and various countries have enacted breach notification laws. These laws typically require firms that lose sensitive personal data to provide written notification to all individuals potentially affected, as well as credit monitoring and other services. Yet, even without a legal obligation, most firms now choose to provide this notification voluntarily to protect their reputation.

And irrespective of any legal requirements, clients expect such notification. However, not all cyber-policies cover these costs, so be sure you understand how your policy will respond.

Policies also differ on how or whether they might respond by breaches caused by rogue employees. All policies have a "conduct exclusion" that applies to dishonest, fraudulent, or criminal acts committed by the firm or its senior management. Even though most data breaches result from negligent acts, such as failing to properly configure a firewall, many are caused by malicious acts, perpetrated or assisted by insiders. To make sure they're protected, law firms should seek an exception to the conduct exclusion for "rogue" or disgruntled employees.

Many cyber-liability insurance policies don't cover theft of hardware from the insured's premises. They also may limit protection for breaches to those involving U.S. privacy statutes or regulations, a potential a concern for firms with international operations or clients. Many policies also have inadequate sub-limits for forensics and crisis management expenses, which can leave law firms with inadequate funds to investigate where their systems were infiltrated or to address the costs of managing an incident-related crisis. And other coverage restrictions might apply to restoration of intellectual property or proprietary business information.

Assessing cyber insurance needs. There are no guidelines for determining how much cyber-liability insurance any law firm should purchase, but three considerations can help with those decisions.

First, what's at stake? Firms with significant amounts of personal identifiable information, intellectual property, or highly confidential information either for clients or staff, may need higher limits. There are both first-party and third-party costs associated with a cyber-breach. First-party costs include lost billing time, forensic Investigation, legal fees to determine regulatory obligations, notification, communication, and public relations costs, credit monitoring, and regulatory fines and penalties. Third-party costs include those associated with settlements, damages to third parties, legal fees, damages to network security of a trading partner or vendor, intellectual property infringement, and regulatory proceedings.

Second, determine what costs your firm can retain. Base this analysis on a worst-case scenario. Even firms with sophisticated safeguards to prevent cyberattacks are vulnerable, and recovery costs can be substantial.

Finally, consider your firm's contractual obligations. Clients are increasingly requiring law firms and all vendors to purchase certain minimum limits of cyber-liability insurance.

As internet and cyber-related risks become increasingly widespread and complex, law firms should take a comprehensive approach to manage them. This involves the implementation of sound risk management and careful evaluation of available insurance.

# # #