Understanding the Cyber Risks of Law Firms

November 2013 • Lockton Companies

EMILY FREEMAN
Lockton Global Technology and Privacy Practice
emily.freeman@uk.lockton.com

Many law firms believe that cyber liability risks are already covered by legal professional liability (LPL) or indemnity insurance. While LPL insurance affords some coverage for cyber liability risks, it also includes a number of grey areas as well as specific areas where there is clearly no coverage due to the scope of the insuring agreement, definitions, and exclusions.

It is important to remember, particularly in the grey areas of coverage, that LPL policies were designed to address wrongful acts, errors, omissions, or breaches of contract or duty arising out of the insured firm's professional services as attorneys, counselors at law, or notaries and therefore do not specifically contemplate cyber risks. In the event of a cyber claim, these limitations may, at the very least, give rise to disputes regarding policy interpretation or denials of coverage by the professional liability insurer.

Here are the major reasons why law firms should buy cyber:

- High retention on LPL policies of large law firms versus retentions on cyber policies (which can be as low as $250,000 for major global law firms). Effectively, the retention of a large law firm's LPL policy removes the insurer from all but the largest single civil suit affecting either single or multiple clients.
- Access to the cyber insurer's external resources for legal, forensics, and credit protection services in the event of a data breach, not only in the U.S. but also increasingly in Europe and other parts of the world.
- These resources are important, as data breaches involve immediate response and specialist jurisdiction knowledge, and play out in a manner that is totally unlike the extended legal process of a professional liability claim.
- Coverage for notification, forensics, and crisis management costs (direct costs) are not part of an LPL insurance program.
- Clear coverage for privacy regulatory and payment of civil fines and penalties are not part of an LPL program.
- Ability of Lockton's cyber manuscript policy—using specialist policy wording for law firms—to be primary to the LPL policy and its excess tower.
- Cyber policies cover data breaches where the affected individuals are employees of the law firm anywhere in the world. LPL policies do not address data breaches affecting the law firm's employees, applicants, retirees, and other parties.

LOCKTON®

- Ability of Lockton's cyber manuscript policy to cover client contractual indemnity requirements for data breaches.
- Clear and affirmative language to deal with issues such as outsourcing and employees as perpetrators.
- No coverage with LPL for first-party interruption/suspension of the law firm's computer network, either directly or contingent (outsourced IT/hosting).

To provide background from a liability perspective, cyber risks arise from a combination of security and privacy exposures.

Security

The unauthorized access, exposure, disclosure, use, destruction, or modification of nonpublic, personal, or sensitive corporate, third-party information (both electronic and paper), including the failure to take steps to protect such information from theft by social engineering techniques or failure to secure mobile devices that contain such information.

Law firms are a major user of mobile devices such as laptops, tablets, and smart phones. Security risks must be seen from a technology, people, and processes perspective, including the possibility that trusted employees or trusted third parties with access to the network are potential perpetrators (or may be in league with the perpetrators) of a security breach. This is a major risk for law firms and a complex one, given the variability of law and regulation globally.

Privacy

The violation of ever-evolving privacy laws or regulations that permit individuals to control the collection, access, transmission, use, and accuracy of their personally identifiable nonpublic information. Behavior or practices in contradiction or in violation of the corporate privacy policy is a significant aspect of this risk.

A law firm's exposure to cyber risk is twofold:

1. As a data collector/owner of sensitive information about its employees, including applicants and retirees.
2. As a professional service provider to its clients.

This is an important point, as the key elements of cyber losses—civil liability; privacy regulatory costs; and notification, forensics, and crisis management costs—develop very differently in the role of a service provider versus that of a data owner. Data breaches can create cross-border regulatory investigations, notification obligations, and civil suits as the venue follows the residency of the affected individual(s), not where the breach occurred or where the services were performed. Mandatory notification—required currently in 46 U.S. states and a number of countries, including Germany—has multiple financial and reputational consequences. There is a generally accepted view in U.S. state notification laws that encrypted data is outside of the mandatory notification requirement. In 2014, the EU is moving to implement mandatory notification across all member countries and potentially imposing very large fines based upon global revenues of the parent company. Even in jurisdictions where notification is not required, the common practice has been to provide some form of voluntary notification.

Data breaches can create cross-border regulatory investigations, notification obligations, and civil suits as the venue follows the residency of the affected individual(s), not where the breach occurred or where the services were performed.

Typically, security/privacy civil claims in the U.S. are filed as class actions. But most courts have found that the plaintiffs do not meet the requirement of actual or imminent injury or financial damages. Plaintiff lawyers have turned to the asbestos litigation of the past and are using the legal theory that future harm will likely occur to the affected individuals in the class; and therefore, the case should be certified. Although these classes are generally not certified, the legal costs—both defense and payment of plaintiff lawyers—can run in the millions.

Regulators are active in this area, and insurers are seeing the growth of regulatory investigations and a rise in fines or penalties, including imposition of consumer redress funds.

Law firms may outsource aspects of its legal services, IT, or business process services; security and privacy events may arise out of acts, errors, or omissions of such outside vendors. Although a function can be outsourced, law firms cannot escape its responsibility from a legal and contractual perspective for the data breach.

A law firm's client—as the presumptive data owner—can face significant financial costs and reputation damage caused by a law firm's data breach. Some specific legal practices, like medical malpractice, personal injury, and workers' compensation, involve particularly sensitive personal information. Other corporate practices, like acquisitions and intellectual property, can potentially expose sensitive third-party corporate information. Clients, particularly in high-compliance industries such as financial services, healthcare, government, utilities, and large public corporations, are very concerned from a due diligence and contractual perspective about any outsourcing provider, including professional services firms. Strong indemnity requirements in event of a breach of confidentiality or data breach may be inserted into the client contract with its law firm.

Law firms also face first-party cyber risks to their computer systems, a time-sensitive critical asset. Traditional property insurance covers physical loss to physical things: the data center and computer hardware. Many risk scenarios involving damage to electronic digital assets and network interruptions do not involve physical loss. Also loss of net income arising out of adverse media attention surrounding a data breach is not insured in a property program.

LOCKTON'S CYBER INSURANCE POLICY FOR LAW FIRMS

We do not recommend that any legal professional services firm purchase an off-the-shelf cyber liability product. Lockton has developed a specific manuscript wording for law firms designed to address the particular requirements of the client and the issues involving the presence of some overlaps between the LPL world and the cyber world.

Lockton's cyber insurance addendum policy recognizes the reality that a data breach by a professional services firm in performing professional services will likely trigger a demand on the data breach indemnity in a client contract. Our policy for cyber liability contains an affirmative grant of coverage for a business associate or client contractual indemnity for a data breach.

The wording is also structured to reflect the law firm's executive titles and substantial amendments to defense of a claim section for large law firms that have internal privacy law expertise.

Lockton has been a major initiator of change in the process of securing cyber liability coverage. We host an underwriting briefing conference call for your cyber liability coverage, rather than completing a standard, lengthy insurer IT security application.

Our job is to assist your team in outlining your overall compliance controls and IT security practices. We use the single underwriting conference call with our leading markets (no multiple calls or individual meetings) and require all invited underwriters to sign a nondisclosure agreement to attend the call. We provide specific guidance to help the law firm's general counsel and IT security leader present the firm and its security/privacy posture and controls.

LOCKTON IS KNOWN FOR:

- Our ability to design the broadest, customized risk-transfer solution in respect of cyber risks for law firms with a specialist team (Lockton's Global Technology and Privacy Group).
- Our ability to provide risk management advice and support, including recommendations for best practices.
- Our commitment to you that our most senior and technically proficient Associates will design, market, and implement your cyber program, including our support in the event of a security or privacy breach.
- A clear and concise implementation plan to obtain cyber insurance.
- Our market leadership on new coverages, including first coverage for loss of computer networks, whether direct or contingent (outsourced IT/hosting).

www.lockton.com

g\whitepaper\freeman\2013\freeman_cyberforlawfirms_nov2013_4pgs.indd