SOMPO INTERNATIONAL
INSURANCE

Discussion Paper: Lawyers Professional Liability Insurance Versus Cyber Liability Insurance

Discussion Paper:
Lawyers Professional Liability Insurance Versus Cyber Liability Insurance

Over the last few years, law firms have been making significant investments in network hardware and software for the operation of their business, including the protection of client data. There is now also increased interest by law firms in purchasing Cyber Liability Insurance, primarily in response to increased scrutiny by clients as to what steps they are taking to improve security of data. In some cases, clients will even audit law firms to ensure compliance with their required standards. Buying Cyber Insurance can provide clients comfort that data security issues are being addressed since insurers have an interest in learning what steps are being taken to mitigate the risk for claims that could fall within the terms of the policy. In addition, Cyber Insurance provides a source of recovery in the event the client incurs financial loss due to a data breach emanating from the law firm.

A second driver for these investments is reputational risk and the belief by law firms that loss of client confidence could have significant negative consequences. Of course, law firms have always had an ethical obligation to keep their clients information confidential and secure; indeed it is the cornerstone of the attorney-client relationship and the advent of the internet has not changed those duties. What has changed is the ease by which large amounts of data can be stored, managed and transmitted, and the increased opportunities for third parties to steal information.

Insurance for Cyber Risks

Cyber exposure risks can be divided into two parts – those claims that arguably fall under the scope of Lawyers Professional Liability (LPL) Insurance policies and those that are more appropriately addressed by specific cyber policies. LPL policies, subject to their terms, conditions and limitations, are designed to cover claims brought against the firm arising out of the provision of professional services, primarily to clients or other third parties to whom the firm owes a duty arising from such professional services. With a few exceptions, most LPL policies offered by insurers do not contain any specific cyber liability exclusions. Therefore, claims could arise out of the failure to protect confidential data from intentional threats or inadvertent release of data. It could be argued that a duty of care in the protection of confidential client information goes hand in hand with professional legal services provided by the firm. That said, the policy is not designed for first party losses and certain other areas of risk for which Cyber Insurance may be more appropriate.

Cyber Liability Insurance can include cover for:

- Unauthorized access, use or disclosure of confidential information
- Participation of an insured's network in a hacking event or denial of service attack
- Business income and contingent business income losses
- Digital asset (data) loss, such as that resulting from a lost or stolen laptop
- Network or data-oriented extortion threats
- Privacy breaches caused by employee's use of their own mobile devices for business purposes
- Regulatory actions including fines and penalties
- HIPAA fines and penalties

- Costs arising from breach response, PR expenses, and forensic investigations
- Losses caused by the firm's vendors such as IT management services, e-discovery consultants, contract attorneys and sub- contractors, and co-counsel

Why Should Law Firms Buy Cyber Insurance?

Even if elements of cover exist under an LPL policy, there are many reasons to purchase separate Cyber Insurance.

- Contractual Requirements. Today many corporations are requiring vendors handling sensitive information to provide proof that they are carrying certain minimum limits of Cyber Liability Insurance to guarantee some degree of financial protection in the event the third party compromises their data. Financial institutions and healthcare institutions are particularly likely to require Cyber Insurance and apply this to their law firm advisors.
- Independent Assessment. Securing cover means a firm must undergo a review by a third party, typically a cyber liability underwriter, of their systems and procedures and be approved as an acceptable risk.
- Breach Response Vendors. Cyber Insurance typically provides pre-arranged access to vendors who can provide immediate assistance in the event of data breach.
- Response Time. Cyber claims require a response time from insurers measured in hours, whereas LPL policies which typically involve many insurers acting through representatives take days and sometimes weeks to evaluate the claim, decide on coverage, and implement a recommended strategy. By this point it's too late, as action often needs to be taken immediately to meet State Attorney General and other regulatory deadlines.
- Claims Not Covered by LPL. Cyber claims which may not be covered under an LPL policy include:
  - Data breach that may not involve client claims nor be associated with any client services,
  - Claims by third party vendors,
  - Claims brought by employees due to disclosure of their personal information,
  - Claims for fines and penalties,
  - Losses incurred by threats from third parties to cause material harm to the firm or their clients,
  - Loss of firm revenue caused by a disruption to the firm's services by employees or third parties committing a hostile act to the firm's systems, and
  - Emergency breach response expenses covering legal specialists, forensic investigators and others to determine exactly what occurred, what data if any was compromised, and what regulatory requirements may need to be met.
- Low Cost Additional Coverage. Firms can buy Cyber Insurance at relatively low cost and for retentions normally a fraction of the amount required by LPL insurers. Further, purchasing a policy that is specifically designed for cyber risks avoids disputes as to what is covered by LPL insurers, some of whom may not be inclined to respond to these risks. If an LPL insurer does pay a loss for cyber risks, it would impact not only limits that are available for other LPL claims but also the LPL premiums.

Interrelationship between a Cyber Liability Policy and a Lawyers Professional Liability Policy

There is every likelihood that a cyber claim will fall within the ambit of both the Cyber Policy and the LPL policy. This overlap could be managed through an endorsement amending the LPL policy.

1. The LPL policy would respond after the Cyber Policy, which would be primary to the LPL Policy for cyber claims. As a practical matter in the event of first party losses, such as breach notification, the loss would need to be addressed immediately, which is better accomplished through cyber coverage. If handled well, a prompt and thorough response could mitigate a malpractice claim.

2. Typically the LPL policy would have retentions larger than the Cyber Policy and normally it must be self-insured so the insured must expend an amount equal to the retention without contribution from other insurers before the policy responds. We suggest an endorsement that not only acknowledges the existence of the Cyber Policy but specifically provides that any amount paid within the retention of the Cyber Policy or by payments under the Cyber Policy count towards the erosion of the LPL retention but only to the extent such payments would have been covered under the LPL policy. For example, costs for breach notification or other first party losses would not count but a third party cyber claim arising out of covered professional services would.

3. Once the retention under the LPL Policy has been pierced the policy would pay excess of the Cyber Policy. Notification of such a breach would be given to both sets of insurers.

Having the same (lead) insurer on both the Cyber Policy and LPL would certainly reduce the potential for gaps between the policies. In addition, there must be strong cooperation in the handling of the claim between the insured and insurers. It would be helpful if both insured and insurer agree in advance on a lead coordinator within the insured responsible for all aspects of the breach response as well as service providers, particularly for first party cyber claims.

For more information on Lawyers Professional Liability Insurance contact:

Stuart Pattison	*+1.917.281.0744*	*spattison@sompo-intl.com*
John Muller	*+1.917.421.4961*	*jmuller@sompo-intl.com*
Dennis O'Connell	*+1.212.209.6524*	*doconnell@sompo-intl.com*

For more information on Cyber Liability Insurance for law firms contact:

Brad Gow	*+1.917.281.0740*	*bgow@sompo-intl.com*