## CYBER INSURANCE AND LAW FIRMS

Cyber insurance has been developed to respond to a number of the financial risks arising out of the failure to protect valuable data. It is important for law firms to note that the potential for financial harm goes beyond damage to clients and consequently there are exposures that will not be picked up by a Lawyers Professional Liability policy.

The financial harm that can arise out of data loss depends on what kind of data has been lost, and how the data has been lost. For the purpose of this discussion it's important to define a couple of terms, in particular "loss" and "data". By "loss" we mean that a firm has lost control over data – through, for example, a lost mobile device, inappropriate access, unauthorised disclosure, theft, network damage denying or restricting access to data. In terms of potential financial harm and available insurance, we can broadly put data in 2 categories – "business critical data" and "personal data".

Business critical data - this data is essential to operate as usual and perhaps in order to maintain a competitive edge. This kind of data is very broad - client lists, proprietary software, a firm's own intellectual property, client confidential data, a document management system, a client relationship management system or billing systems.

Personal data – this is personal information of Private Clients, employees, partners, ultimate business owners or for example members in a collective action or individuals linked to the subject matter of a law suit (investigators, prosecutors, defendants). Any firm that collects, processes or stores personal information could be exposed to numerous international privacy laws & regulators.

## POTENTIAL FOR FINANCIAL RISK BY TYPE OF DATA

### Business Critical Data Loss

If a law firm loses the details of a corporate transaction or client intellectual property, the direct consequence will almost certainly be the loss of that client and liability for the breach of confidentiality.

The Lawyers Professional Liability minimum standards wording in England & Wales provides broad form negligence cover. There is no exclusion for breach of contract, breach of confidentiality nor is there an exclusion for the wrongful acts of insiders provided there is no senior level knowledge of the wrongdoing. Unless or until forms change, we think there is a strong case for claims for data loss *liability* under such a Lawyers Professional Liability policy.

If data has been lost through a hacking event of, for example the document management system, the system may be damaged or other data may have been corrupted. Lack of access to the system or data therein may impact a firm's ability to deliver services to other clients which could result in indirect Loss of Income. In order to get services running again, a firm is looking at Extra Expenses:

- to hire external experts to assess the scope & cause of the network breach
- to hire external experts to remediate the weakness;
- the increased cost of doing business because employees and management are distracted by the breach from their usual work; and
- to rework or recreate data that may have been corrupted.

There would be no claimant for Extra Expenses, so the LPL would not be triggered. Some coverage for systems damage may be available under a property policy. We are not experts on property insurance, so can not speak about the scope of cover with authority, however, we understand that property typically covers physical assets; "data" is considered non-physical and therefore it is unlikely to find coverage for damage to data under a traditional property policy.

Personal Data Loss

The same exposures apply to the loss of personal details as discussed regarding lost business critical data but you can add the complexity of exposure to newly empowered Regulators, we all know the cost of these can only go one way. In certain situations, a firm may be required by law to provide Notification to the relevant data authority and individually to the data subject. If a firm is the data owner of data of a US resident, it must comply with the state law where the data subject is resident. Privacy laws in other countries may be triggered because data is stored or exposed in that jurisdiction.

Again, we would look first to the LPL for liability to clients; however it is worth pointing out that the LPL would not extend to claims brought by employees and partners. Coverage may be available under an Employment Practices Liability policy, if not coverage for claims brought by employees for breach of privacy is available under a Cyber policy.

Privacy Regulators are staffing up and have been assessing fines and enforcement actions; in the US we've seen one state attorney become a senator after winning a landmark privacy case. In the UK, the recently empowered Information Commissioners Office has been busy assessing fines, including the recent fine against the now defunct firm ACS:Law a law firm that had specialised in Intellectual Property for failing to keep the personal data of at least 6,000 people secure. The ICO would have fined ACS Law £200,000 had the company still been trading.

LPL policies exclude fines and penalties. Many Cyber policies provide affirmative coverage for Punitive Damages and Regulatory Fines and Penalties, where insurable. Defense coverage for regulatory actions is also available.

Cyber insurance is a hot topic in America, and this trend is largely driven by the Notification requirements in Forty-six states, the District of Columbia, Puerto Rico and the Virgin Islands. For the data owner, Notification costs are a direct calculable cost for which there will be no "claim" and therefore no coverage under an LPL policy. Cyber policies were designed to cover Notification costs.

Notification outside the US is not consistent though several countries have similar requirements, such as Canada, Mexico and Germany. Several countries require notification to the relevant Data Authority, who in certain circumstances may publish the notification on their website thus taking what had been a private matter into the public domain.

Data loss is not a new issue; it's just that we are hearing a lot more about it now. The publicity of data breaches and the inconsistencies in law with respect to Notification pose challenges to a firm's Reputation.

What is a multinational firm supposed to do when a data loss impacts individuals in territories with notification laws as well as those without? Sony wanted to treat all their customers equally and to provide everyone the opportunity to take the same financial precautions. They went above the required response by volunteering to notify their 77m account holders of their *first* data breach, at what has been estimated to be $20.00 per notification, and are being roasted for doing to little too late. Even the best of intentions can get punished...

Summary

We view the uninsured exposure for a law firm's loss of business critical data to be 1) Reputation, 2) Loss of Income, and 3) Extra Expenses. Cyber insurance provides affirmative coverage for Reputation Crisis Management Costs, Extra Expenses and Loss of Income resulting from systems damage as a result of a security breach.

We view the uninsured exposure for a law firm's loss of *personal* data to the same as with loss of business critical data as well as 4) Regulatory Fines & Defense and 5) Notification costs.

We think some of these exposures can be covered by a Cyber insurance policy. Cyber insurance provides affirmative coverage for:

Public Relations crisis management expenses to mitigate reputational damage

- Extra Expense (increased cost of working, data restoration, systems repair)
- Costs incurred as a result of a Regulatory investigation regarding the loss of personal protected data: Defense, fines & penalties where insurable
- Notification Costs including the legal costs to determine the required response & administrative / confirming addresses, printing & mailing letters
- Loss of Income resulting from systems damage as a result of a security breach



For further details or if you have any questions please contact.

Lyndsey Bauer

Senior Vice President

t: (011) (44) 20 7280 8228

e: lbauer@paragonbrokers.com

Tom Quy

Cyber Liability Broker

t: (011) (44) 20 7280 8252

e: tquy@paragonbrokers.com