LEGAL RISK LLP
SOLICITORS

Should we buy cyber cover?

FIRST PUBLISHED IN LAW SOCIETY'S LEGAL COMPLIANCE BULLETIN

'As Benjamin Franklin said, by failing to prepare you are preparing to fail.'

With the government figures reporting 2.5 million incidents of computer crime, including hacking and viruses, and the news full of bank scams and cyber-attacks on law firms, SRA warnings, and insurance brokers selling cyber cover to firms renewing their professional indemnity insurance, the question has to be asked, 'Should we buy cyber cover?' Many insurance brokers have been offering policies in conjunction with the professional indemnity renewal.

If you were expecting a binary yes/no answer to the question of whether you should buy, regrettably it is not that simple, but read on to find out why, and what you need to consider.

Where to start

As Benjamin Franklin said, by failing to prepare you are preparing to fail.

As with any other decision on whether to insure, the starting point is to –

- identify the risk;
- identify how far you can manage the risk;
- decide how much of the residual risk you are prepared to carry yourselves; and
- transfer the risk which you are not prepared to carry yourselves – by buying insurance, if you can find the cover you want at a price you are willing to pay and can afford.

Identify the risk

ACS Law was a firm of solicitors which pursued tens of thousands of individuals for allegedly infringing copyright by sharing pornographic files. On 21 September 2010 ACS Law's website was hacked and the names of the individuals entered the public domain; since then, it has been said that the information on which they relied was inaccurate.

ACS Law collapsed in the aftermath of this. The Information Commissioner ordered ACS Law to pay a £1,000 monetary penalty, but said the penalty would have been £200,000 if the firm had still been trading. The firm was criticised for having computer security barely adequate for home use, let alone a business handling sensitive personal data. The Solicitors Disciplinary Tribunal suspended the sole principal for two years and ordered him to pay £76,326.55 costs.

Since then, we have seen firms suffering a variety of other losses or potential claims. Some have been attacked with ransom software such as CryptoLocker denying access to their systems unless they pay a ransom.

Others have had their emails hacked and been duped by spoof emails into paying money to fraudsters, either their own money or client money. Examples of this have been fake emails from clients saying they have changed bank accounts and asking for the proceeds of sale of a property to be paid to a new account.

NetDiligence's latest cyber claims study reported that smaller organizations with revenue of less than $50 million accounted for 28 of claims.

If you were the victim of an attack, would you know where to obtain help? What help would you need? You may need assistance with IT, or advice on litigation to freeze assets and recover the money, or specialist public relations advice. You may need to inform clients if you have lost their data, such as credit card information, and there may be the cost of credit monitoring.

These are just a few examples. Some firms may represent higher risk than others – personal injury firms hold vast amounts of sensitive personal data. Firms which are advising on litigation against banks will hold account information which may make them higher risk.

Identify how far you can manage the risk

If the Pentagon can be hacked, as it has been, and the Russian Federal Guard Service has felt the need to buy typewriters, law firms clearly cannot eliminate the risk. It is unlikely that law firms can protect themselves against hacking by sovereign states.

The stakes can be high. On 31 January 2012,

Bloomberg reported that China-based hackers looking to derail the $40 billion acquisition of the world's largest potash producer by an Australian mining giant hacked seven Canadian law firms.

But there are steps we can and must take: the seventh data protection principle requires that 'Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data'. Outcome 7.5 in the SRA Code of Conduct requires compliance with data protection legislation. Chapter 4 of the Code imposes obligations to keep client material confidential.

More important for most firms, though, will be the need to protect their reputation: as law firms, our reputation is all we have to sell.

How sophisticated the technical measures to prevent cyber-attacks are will to some extent be determined by the firm's size and resources but some should be a given in any firm, such as antivirus, firewalls and encryption of mobile devices. Some measures may be highly sophisticated, but many may be relatively simple to implement. See for example the Government's '10 Steps to Cyber Security'. Remember that some do not even involve the application of technology – one of the key risks is staff - not only current staff but recent leavers, who may have security information which is sufficiently up to date to be of value.

Realistically you need relationships in place already – it is the same as if a pipe bursts on Saturday night - unless you already have the number of a plumber and know they will come out, you will struggle to secure the services of one. It is probably too late to start looking in the Yellow Pages.

A significant portion of the risk arises from one's own staff, including disgruntled employees and recent leavers who still have inside information which is sufficiently current to be of value. Even innocent employees are a risk, as they may have been targeted through social engineering. Training is key to the prevention of many of the attacks to which law firms are exposed. No firm is immune from attack – we have seen high value attacks, some successful, on global firms, high street firms, and those in between. Online training is not expensive, need not take much staff time, and may pay for itself thousands of times over.

Decide how much of the residual risk you are prepared to carry yourselves.

This is linked to the next item, but you do need first to identify the security measures which you can implement, under the last heading, and the cost of implementing them, before moving on to the question of whether you buy insurance, and what insurance you buy.

You also need to bear in mind that some losses may not be insurable; fines and penalties in particular may be an issue here, though some policies do cover regulatory fines (where the law allows).

Transfer the risk

Insurance is the last link in the chain. It may present opportunities to help you manage the risk in two ways. First, it may cap your financial risk. Secondly, it may provide emergency services to which you would not otherwise have ready access.

You need to consider what insurance you have already: the compulsory professional indemnity cover under the SRA Minimum Terms and Conditions in effect covers client claims, but a separate policy (with appropriate wording) may help you protect your professional indemnity claims record and may be subject to a smaller excess. You may have business interruption cover under your office policy. Some professional indemnity policies have cyber extensions – but may only provide limited cover.

Unlike professional indemnity, where all insurers offer broadly similar cover under the SRA Minimum Terms and Conditions (for another year, though that may not survive the next round of SRA reform), there are wide variations in cover, as this is an emerging market. It is therefore essential that you give detailed attention to the policy wording and look at several insurers' offer-

ings before you buy.

What can you insure?

The first question is what do we mean by cyber risk? Many of the press reports in articles under this heading involve frauds perpetrated with nothing more technologically sophisticated than a telephone – so-called 'vishing' attacks, with callers pretending to be from the bank and duping a solicitor or member of an accounts team into provision of pass codes or persuading them to transfer money to an account which is not under their control.

These may not fall within the scope of a cyber policy. As it is early days for cyber policies, there have been few examples of coverage disputes between insurers and insureds, with no reported cases in this country so far as the writer is aware, and only a small number of cases in the United States of America.

In one such case, a health insurer had a computerised billing system that allowed health care providers to submit claims directly and most of these were paid automatically, without manual review. The insurer claimed that it had sustained $18 million in losses for fraudulent claims it paid that were submitted by providers for services that were never rendered. This was held not to be covered, because the entries on the system were made by authorised users, rather than hackers.

Another case, however, went the other way. This involved a fraudster calling to ask the insured to change account details for payment of a genuine supplier's bill and $2.4 million was diverted to the fraudster's account. In this case, the court held that cover applied.

Much turned on the policy wordings, which were different in each case, but the cases do highlight the need for detailed consideration of the policy. There have been many cases of law firms sending client money to a fraudster following a fake email notifying the purported change of the client's account details.

The policy

It is also important to ensure that the policy is suitable for a professional services firm – some may be more tailored to other sectors, such as internet sales. There will be policy limits for each head of cover and you need to check they are sufficient for your purposes. As with any commercial document, you need to look carefully at the definitions: one policy, for example, contains a definition which has the effect – perhaps not obvious at first sight – of excluding claims where the perpetrator uses the firm's hardware.

While the SRA Minimum Terms and Conditions give wide protection in relation to professional indemnity policies, such as protection against the consequences of non-disclosure, there is no such 'gold standard' for cyber policies which are subject to normal commercial terms: cyber insurance is an emerging industry.

While the Insurance Act 2015 will bring in some added protection next year, it is critical that the buyer understands the product they are buying. The policy may, for example, contain warranties as to the firm's security systems, such as firewalls and anti-virus, but could your insurance protection be lost if a partner or employee is working on their own computer at home? Does the policy require you to maintain certain security standards and can you comply with the requirements? Software updates are often critical – 'install and forget' is no longer acceptable and your patch management policy can be a critical part of your defence against malware.

Policies may be replete with exclusions, as insurers are getting to grips with modelling their exposure, and particularly the aggregation risk to which they may be exposed by a single malware attack affecting their entire book of business.

Note too, that the policy may contain a retroactive date, excluding liability for claims arising from incidents before a particular specified date. A report by Santam on the South African market noted that it takes approximately 200 days for a South African company to identify an online security

LEGAL RISK LLP
SOLICITORS

breach; there is no reason to think that may differ significantly from elsewhere.
Policies cover two broad types of risk – the firm's own losses (or first party cover), for example, damage to computers caused by hackers, and claims by clients and others (third party cover).

First party cover

Your system has been hacked, nobody can do any work, there are key dates, hearings, completions… What do you want to happen next? This may be where your troubles start, whether you have cover or not.
If you rely on external providers for IT support, your first thought is probably to ring them, ask them if they can drop everything and come round and sort out the problem. They know your system inside out, and in most cases are probably best placed to sort things out and have the system, or a replacement, up and running as soon as possible.
The policy may cover the costs of restoring data, systems and hardware, but if you want to claim on your cyber policy, however, you will have to follow the claims procedure, which may involve a third party such as loss adjuster, and will probably have to use their IT providers. When you choose your policy, you need to understand what this might involve in terms of process and timescales.
Business continuity may or may not be covered. Check whether your office policy covers this, and what the exclusions are.
The policy may provide crisis management advice, including forensic support, and assistance in protecting your reputation. This may bring much-needed expertise to help manage the process and start putting things right.
Policies may provide cover for the cost of notifying clients. However, one policy the writer reviewed for an English firm restricted this to cases where this was compulsory under US law(!)

Third party cover

Policies will generally cover claims and defence costs for claims arising from unauthorised access to systems resulting in privacy breaches. There is also the risk of transmitting viruses or malicious code to consider. Liability may also arise from inability to access systems.
The aim is to reduce the risk of claims on your professional indemnity policy and obtain a smaller excess, but as mentioned above, you need to consider how this interacts with your professional indemnity policy in order to avoid double insurance (which would involve liability on both policies and an excess on each).
Privacy liability cover would assist in responding to claims arising from unauthorised access to, or wrongful distribution of, personal data, which might, for example, include identity information. This may include the cost of credit monitoring.

So…should we buy cyber cover?

The answer really depends on your ability to manage risk and willingness to carry risk. But for many firms, their answer may be a cautious 'yes' – provided they understand what they are buying, what is covered and what is not covered.

16 October 2015

Frank Maher is a partner in Legal Risk LLP, solicitors, specialising in advice to law firms on professional indemnity and other insurance and professional regulation. *www.legalrisk.co.uk*