Cybersecurity:
what are insurers looking for?

Nicola Laver investigates how law firms can satisfy their insurers that their cybersecurity and anti-commercial crime strategies are robust.

About the author

Nicola Laver is a freelance legal journalist/editor, and a former solicitor.

Given that research has shown that cyberattacks on UK law firms increased by nearly 20% between 2014–15 and 2015–16, robust cybersecurity strategies are vital issues; furthermore, 73% of the top 100 law firms in the UK were the target of attacks last year.[1]

Common cybersecurity threats law firms face involve phishing attacks to gain access to client money. Other serious incidents highlighted in the research include infection by viruses or malicious software; loss or leakage of confidential information by staff; significant attempts to break into the firm's network; and denial of service (DOS) attacks.

These results suggest that law firms are not taking sufficiently robust action to protect their firms and clients from cyberattacks: add the fact that cybercriminals are notorious for staying one step ahead of the game – it is clear that firms cannot afford to be complacent.

Are firms taking cybersecurity sufficiently seriously?

Colin Tankard, managing director of Digital Pathways, a specialist company in the cybersecurity and protection industry, says that the majority of large law firms are taking data security seriously and have introduced strong controls on users and document management. 'However,' he adds, 'medium to small firms are still relying on third parties to handle their data security who, in many cases, are not skilled in the area, or who recommend solutions which do not fully address the specific risks law firms face.'

He says that Digital Pathways has seen companies that handle telephone systems, installing and managing data security systems. 'This is like asking a GP to handle brain surgery rather than a neurologist, both are medically qualified but one has specialist knowledge and skills'.

Law firms need to think about using specialists rather than taking a 'one-size-fits-all' approach, thereby benefitting from 'best-of-breed' technology, with a separation of responsibilities. This, says Colin Tankard, can dramatically increase the level of data protection.

Andy Bugby, lead underwriter at RSA, is a specialist in cyber risk and commercial crime insurance. He says that while there is a growing awareness of cyber issues, his opinion of the legal profession right now is that this has mostly been focused on client funds (this is traditionally covered by professional indemnity insurance (PII)). He adds: 'The area that the sector is playing catch up on is some of the live cyber issues that are out there. We are all playing catch up on those issues because cybercriminals are very clever and will come up with new things every day.'

What firms do need to keep an eye out for, says Andy Bugby, are 'attacks via malware or extortion attempts: where a virus is transmitted or a criminal will block access to a system, and then demand a ransom payment to be able to reaccess the system. Nothing can be done: the whole thing is blocked, and there are costs in dealing with that. In the absence of firewalls, something like this can get through.

'There are also DOS attacks: somebody who may be disgruntled with the firm, or even a competitor, could flood someone's servers with so much information that the system goes down. Anyone who wants to undertake a DOS can buy

continued on page 14

that kind of software on the internet for as little as £50. These are the key things from a pure cyber point of view.'

He adds: 'The other thing to be aware of, from an insurance point of view, is that a lot of people equate cyber with financial losses. Many products out there will badge themselves as 'cyber', but will do different things. It could be data liability to third parties, or the upfront costs of dealing with a cyber incident. Some policies - the best policies in my opinion - will cover loss of money due to a cybercriminal attack.'

What are insurers looking for?

Cyber and fraud risk management controls

Firms must have robust strategies and procedures in place, and keep them under constant review. Insurers, typically, look for strong cyber and fraud risk management controls, says Andy Bugby, starting with physical IT protection in the form of firewalls and anti-virus and malware protections.

He highlights the government-approved programme, the Cyber Essentials Scheme, which raises awareness of cyber risks and how to manage them.[2] He says that insurers view a firm undertaking this - or a similar programme - positively.

'The second aspect', says Andy Bugby, 'is the firm's people.' 'Fraud and cyber training should be part of a firm's training programme. A culture of checks and challenge should also be promoted, ie, would someone in an accounts team feel confident flagging or challenging a suspicious e-mail asking for a money transfer? Dual controls and sign offs for transactions are also an effective tool here.'

Password security

The issue of passwords crops up frequently in any discussion on cybercrime, because everyone uses these every day. However, Colin Tankard warns firms about the sharing of credentials and passwords. 'Often,' he explains, 'these are shared for very valid reasons but are infrequently changed thereafter, so it's easy for others to log back in to access data which, in normal terms, should not be allowed.' 'We recommend that organisations use two-factor authentication methods, such as one-time password generators on a smartphone, to avoid the password sharing issue.'

Outsourcing the IT function: pros and cons

A further issue is the outsourcing of the IT function. Third parties then have access to all the data and, says Colin Tankard, as law firms tend not to separate the responsibility of duties, they do not control what a third party can see or do. He says: 'This is rather like the Snowden [Edward Snowden is an American computer professional, and a former Central Intelligence Agency employee and former contractor for the US government, who copied and leaked classified information from the National Security Agency in 2013] and the Pentagon hack of data. We recommend firms add access rights to a user's credentials, so that they can allow an administrator to manage tasks, such as backups, but block the administrator from opening and viewing the content of an individual document.'

Colin Tankard says that specialist data security companies should be employed, not companies that provide, for example, case reference systems or other IT-related, but not specialist, services. He says: 'Whilst the 'one-throat-to-choke' approach might be cost effective, it often provides weak areas of service outside the key product.'

User-monitoring software

User-monitoring software, which triggers when a user attempts to view a folder or begins a process that could damage the organisation, can also be useful. Colin Tankard says that this educates users into good practice, and will reduce the amount of data leakage, either malicious or accidental. He warns that law firms are not yet embracing document and e-mail security, and firms must take steps to protect sensitive communication.

Terry Seager, director of Hera Indemnity, highlights the questions insurers tend to ask, in the context of crime risk and exposure, to which law firms should be able to answer: 'Yes' (see box on page 18). He adds: 'To ensure the very best consideration and preferential terms, they should go a little further than this and demonstrate that there are checks and balances embedded in their processes to try and overcome the 'human factor', for example, a block on the transfer of funds without client and account verifications checks having taken place.

'That said - a firm should avoid deluging insurers with information. A letter setting out the salient points, and making reference to a procedures manual, is likely to get a better reception than the procedures manual itself as insurers have limited time to carry out the risk assessment.'

What do firms need to do now?

By taking the right steps now, your firm can minimise the risk of cyberattack and satisfy your insurer. Colin Tankard advises firms to have a vulnerability assessment of their network carried out, including a penetration test, which would identify areas of weakness, such as poorly patched servers or bad password management.

From this assessment, a gap analysis can be taken - and steps implemented - to bring the firm into line with industry best practices. He adds that the information gleaned would ensure that, in the event of a breach of the PII cover, insurance terms would not be negated due to lack of data controls.

continued on page 16

What impact will the General Data Protection Regulations have?

From 25 May 2018, the General Data Protection Regulations (GDPR) come into effect in the UK, requiring all businesses to take appropriate steps to control and protect personal data. To make an insurance claim following a data breach, firms will need to prove that they have taken steps to protect the data.

Colin Tankard says that, as a minimum, data must be encrypted: 'If a law firm cannot demonstrate persistent steps to secure their data, the insurance will not 'kick in' and, in fact, might trigger a data investigation by the ICO [Information Commissioner's Office].'

Breach of the GDPR could result in serious sanctions (4% of global turnover or €20m, whichever is the greater) and, says Colin Tankard, could open up multiple litigations against the firm from any individual who has had their data exposed. He comments: 'Under GDPR, any individual can request a free subject access request, which must be complied with within 30 days. Therefore, the ability to track all PII data must be undertaken in order to meet this requirement. If not done, I suggest that it would not only breach GDPR, but could also revoke any PII cover.'

Other risk management concerns

That said, insurers do recognise that there are particular problem areas for firms, not least the reality that cybercriminals are extremely adept at staying one step ahead. Andy Bugby explains: 'It can be expensive and time-consuming to contact all data subjects, provide satisfactory remedies, and guard against potential law suits and adverse publicity. Recent legislation will soon make notification to the regulator mandatory in loss of data incidents.'

Smaller law firms may lack the capacity and resources to look at all the control mechanisms available. However, Andy Bugby says that risk transfer is available in the form of insurance products.

Colin Tankard says that law firms are also at higher risk of the 'man-in-the-middle attack' because, while they communicate with many third parties and private individuals, they may not be protecting the communication paths enabling such attacks to be intercepted and redirected or changed. He says: 'It is often lack of knowledge that allows this to happen and, in many cases, laziness of individuals within a firm who are not being watchful of whom they are communicating with.'

Terry Seager points out that cyber risk and crime insurances are triggered by an event, and may cover both first and third party losses, whereas a PII policy responds primarily to negligence on the part of the insured which lead to third party losses. He comments: 'There is, however, something of an overlap, and the existence of cyber risk and crime insurance demonstrates active consideration and management of the exposures and, as such, would also be seen as a positive risk factor by professional indemnity insurers.'

QUESTIONS YOUR INSURER WILL ASK

Terry Seager is a director of Hera Indemnity and a specialist in PII. In Hera's experience, many professional indemnity insurers are increasingly focused on cyber risk and crime exposures as part of their own deliberations, and insist on a basic question set. They will not confirm a quotation without this information.

- Has the insured taken steps to implement fraud guidance measures, such as those provided by CILEx Regulation Limited and the Solicitors Regulation Authority?
- Has the insured trained all staff involved in handling funds on effective methods of verifying the identity of clients and bank account details, and does this include a two-stage ID process (such as calling a client on a known telephone number to verify e-mail instructions)?
- Does the insured ensure that all security software, including anti-virus, anti-spam and firewall software, is regularly reviewed to ensure the detection of malware and is all software regularly 'patched'?
- Does the insured exclude liability for fraudulent or malicious e-mail that purports to come from them, and make their clients responsible for ensuring that all e-mails from the insured are genuine before acting or relying on them?

Robust protection is key

As the Law Society states in its guidance on cyber insurance: 'Protection and prevention should be your firm's priorities to guard against damaging cyber-attacks. Insurance is not a substitute for good system protection.'[3]

Cyber insurance should be an additional safeguard to cover certain costs and losses in the event of a data breach and or cyberattack affecting the firm's computer systems.

Demonstrating that you are maintaining robust protection of your firm from cyberattack is vital: not only in terms of your regulatory responsibilities, but also from the insurer's point of view. Complacency is simply not an option given that cybercriminals strive to stay one step ahead of law firms.

1 *25th Annual Law Firms Survey 2016. Executive summary. Standing the test of time: 25 years of the Law Firms' Survey*, available at: www.pwc.co.uk/industries/business-services/law-firms/survey.html
2 Visit: http://tinyurl.com/o8jrgbj
3 'Cyber insurance guidance for law firms', available at: http://tinyurl.com/l2pykxq