MARSH JLT SPECIALTY

INSIGHTS | MARCH 2021

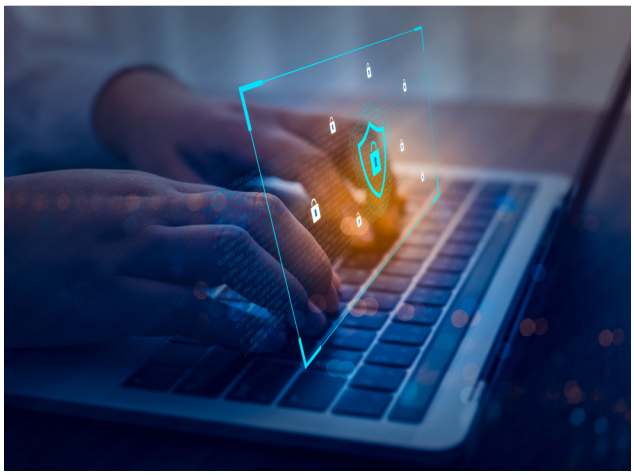
Risk Dimensions Newsletter

Welcome to the third edition of our law firm newsletter. In February 2021, we sent a risk alert concerning an uptick in cyber crime. In this edition, we cover recent cyber crime scenarios and what law firms can do to reduce potential attacks. We also highlight the emerging insurance landscape and examine possible implications.

Cyber crime – the modern risk

Guest contributor Joe Bryant, Partner at Beale & Company Solicitors LLP, writes about the ways fraudsters are targeting law firms, and the protections firms can put in place to mitigate against such threats.

Phishing, whaling, baiting...over recent years these angling terms have become synonymous with cybercrime, with fraudsters casting their nefarious lines far and wide in the hope that something will be lured into taking a bite. Whilst these practices have historically been the preserve of banks and financial institutions, cyber criminals are now increasingly focusing on the legal profession and its insurers to fill their nets.



Quite simply, fraudsters have cottoned onto the fact that lawyers handle client money. Lots of it. The legal profession's focus on safeguarding it, whilst vigorous, is nowhere near as acute as it is in the financial sector, which makes law firms a very attractive target.

The Solicitors Regulation Authority's (SRA) 2020 thematic review on cyber security[1] highlighted the frequency, and potentially hugely damaging consequences, of cyber crime on law firms.

The review looked at 40 firms who had reported being the target of cyber crime over the previous three years. It revealed that cyber criminals were successful in their attacks against over three-quarters of targeted firms, leading to over £4 million of client and office money stolen. Of that sum, £3.6 million was repaid to firms by insurers, but £400,000 was left uninsured and had to be met out of firms' own resources.

Away from the sums stolen, cyber attacks can also have significant indirect financial implications, including higher insurance premiums, the cost of management time, and damage to client relationships and overall reputation.

How are solicitors at risk?

Whilst law firms are increasingly being targeted in ransomware attacks such as the one mentioned above, the most publicised cyber crime incident that has been experienced by the profession over the past few years involves the use of social engineering tactics to deceive someone within the firm into paying money directly to the fraudster. The con typically starts by luring someone within the firm into opening an email with attachments that are infected with malware. The malware then goes to work, often over a number of months, observing the user's activity, obtaining passwords, and gaining sensitive information.

1| Solicitors Regulation Authority, Cyber Security – a thematic review September 2020.

MARSH

Then, when the time is right, frequently on a Friday afternoon, just as the firm is preparing to complete its various conveyancing transactions and is carrying significant funds in its client account for the purpose, the fraudster will call the firm pretending to be from the bank and claiming that the client account has been frozen to protect the firm and its clients. Overcome by panic and believing the fraudster, who has used all of the information gathered by the malware to convince the lawyer of the legitimacy of the situation, the lawyer does everything the fraudster asks. Usually this includes giving the fraudster the one piece of information that the malware couldn't obtain; the randomly-generated code that the bank requires to allow the funds to be released.

This particular modus operandi, of so-called Friday afternoon frauds, has become less popular recently, as firms have wised up to the tactics. That said, we are still seeing a number of cases where the fraudster pretends to be from Amazon or another online retailer and manages to catch the firm off-guard that way. In the place of Friday afternoon frauds, email manipulation frauds have emerged, where the third party fraudster uses its malware not to gather a portfolio of information upon which to base a distressed call but, instead, to look for transactions that are about to involve a transfer of money. The fraudster then introduces another piece of software to intercept all outgoing and incoming email traffic on that matter and then manipulates it, changing either the client's or the law firm's account details so that the victim ends up paying the proceeds of the transaction directly into the fraudster's account, rather than sending it to the legitimate owner of the funds. A very sophisticated fraud indeed.

Measures to prevent these types of fraud are well documented, but are always worthy of further mention:

- Ensure that you have a clearly documented process/reporting line for handling client money.
- Complete all standard anti-money laundering checks in every case.
- Obtain and verify clients' bank account details at the outset of the matter and do not entertain any requests to change those details during the transaction, other than in the most exceptional of circumstances.
- When verifying account details, do so by means other than email or SMS.
- Encrypt all client correspondence wherever possible.

These measures are not fool-proof, and they certainly won't stop fraudsters from continuing to try. Consistent with all of the angling metaphors that abound in this area, cyber criminals rely on casting multiple lines in the knowledge that, whilst most will be ignored, they only need one bite to consider it a successful venture.

With the increase in home working brought about as result of COVID-19, cyber criminals are enjoying a bumper catch:

- Current arrangements have given rise to multiple points of weakness in firms' IT systems, with each individual employee now needing remote access to systems which would previously have been hard-wired to the office desktop.
- Employees now frequently use their personal/home computers for their work activities, giving malware the opportunity to be introduced into the user's personal activities (which are typically far less secure than their professional counterparts) and then infiltrate across into the work systems.
- Employees working alone, away from their teams and supervisors, are also statistically more likely to be susceptible to a successful malware infiltration than if they had been in the office surrounded by their support network.

It is the perfect environment for fraud.

What can be done?

The current situation, which seems to be here to stay, even once offices are open again, warrants a level of vigilance that goes far beyond pre-COVID-19 times. Policies on the use of home computing devices need to be considered and updated. IT infrastructure needs to be maintained to the latest and highest standards, with all patches and anti-virus software installed as a matter of course as soon as it is released. Insofar as firms have not already considered it, secure remote access solutions must be implemented and kept up to date.

Of particular importance is the need for staff to be made aware of the heightened risks through a programme of training, thereby keeping the cyber threat uppermost in their minds in their daily activities.

Needless to say, all employees should already be aware of the risks of handling sensitive data and the firm's code of conduct. They should also know how to create secure passwords, recognise common scams, and safely store and dispose of confidential documents. They should know not to open email attachments from third parties without knowing their origin. They also need to be aware of additional cyber issues particular relevant to home working:

- Firm computers are not for personal use (and vice versa).
- Work files/information should not be copied onto personal devices.
- Firm approved cloud services or data centre storage should be used instead of local storage for files.
- No USB sticks or other personal devices should be connected to the firm's systems.
- Hard copy confidential documents should be safely stored and disposed of.
- The added risks of working away from the office, for example losing paperwork, or having conversations with or about clients that can be overheard.

In any context, employees should be aware that a client requesting payment of monies to a third party other than themselves is also a red flag that something is amiss.

It is important that these cyber security awareness messages are regularly and consistently communicated to all employees to reinforce security issues. Cyber criminals will look to target firms with the weakest defences; often this will be smaller firms where resources may be more stretched and there is less historic investment in IT. But that is not always the case, and some larger firms have neglected their IT security spend in recent years and would do well to review their policies.

What about insurance?

The legal profession's various insurers have repaid millions of pounds in cyber-enabled theft upon their policyholders' client accounts over the past several years, with the threat of SRA enforcement action, due to a breach of the Solicitors Accounts Rules, ever looming in the background. The vast majority of these payments have been made under the auspices of the SRA's Minimum Terms and Conditions (MTC) for professional indemnity insurance (PII). Under the MTC for PII the definition of "claim" has been deliberately broadened over the years to bring client account theft within the scope of cover, in circumstances where one might typically expect that sort of thing to fall beyond the realms of professional liability.

It is perhaps because of the breadth of cover now provided by the SRA's MTC that less than a third of the firms surveyed for the SRA's thematic review held specific cyber insurance.

Most firms seem to feel so well covered by their PII that they assume it will cover all cyber losses. However, with the current changes surrounding silent cyber, discussed in the other article in this newsletter, the breadth of cover will likely shrink.

Also, while cyber-enabled client – that is, third party – losses currently continue to fall within the PII's remit, thefts from the firm's office account will not be covered under a firm's PII, and neither will the indirect losses discussed above. So firms should consider whether their insurance needs extend to such things as:

- Loss of the firm's own money.
- The firm's business interruption losses suffered as a result of a cyber attack.
- Any ransom payments demanded as part of a ransomware attack.
- The costs of rectifying any reputational issues.

Firms should consider purchasing separate cyber and crime insurance cover if these types of losses are of concern. Such polices will provide cover for IT costs incurred investigating, identifying, and preventing cyber attacks as well as the cost of specialist public relations companies to help firms limit reputational damage. Cyber policies will also often cover the costs of specialists assisting in notifying, if required, the Information Commissioners' Office and the affected individuals following a personal data breach. Timely and proper notification can also assist in avoiding or mitigating any penalties.

In the current environment we are all working in, the need to consider these additional protections alongside cyber security measures has never been greater.

Conclusion

Fraud is an ever-present threat to the professional community. Cyber criminality has boomed with the move to online working activity that COVID-19 has brought about. With the home-working trend set to continue long after we are told that we can return to our offices, firms need to keep their security measures, and their insurance protections, under constant review to stay ahead of the fraudsters.

Lots of noise about "silent cyber"

Marsh JLT Specialty's Rachel Evans (Product Development Specialist, FINPRO UK) highlights the emerging insurance landscape relating to silent cyber. She examines what firms should look out for in this evolving area.

Law firms are increasingly dependent on computer systems to provide services, heightening the risk of exposure to cyber crime. Further, an increase in employees working from home due to the COVID-19 pandemic has led to an uptick in vulnerabilities[1].

Two common types of cyber events facing law firms are the theft of client account monies and ransomware attacks. Ransomware is a type of malware that encrypts files and prevents access to a system or data until the victim pays the attacker.

Firms expect their insurance program to protect them against resulting losses and, while insurers try to keep pace with the evolution of cyber risks and their potential exposures, thoughts about where cover should fall for such losses, is a hot topic.

The Prudential Regulation Authority and Lloyd's

In 2017, the Prudential Regulation Authority (PRA) required insurers to identify and measure their cyber exposure through both:

- Affirmative cyber insurance — what the policy explicitly provides cover for.
- Non-affirmative insurance — what has become known as "silent cyber" as the policy wording does not positively affirm or exclude cover[2].

The PRA surveyed insurers to understand how they were ascertaining and stress testing their exposures to cyber events, noting that casualty and financial lines potentially had the largest non-affirmative exposures[3]. In January 2020, Lloyd's mandated that any professional indemnity (PI) insurance placed through it, on or after 1 January 2021, must be clear on coverage for losses caused by a cyber event – by either providing affirmative coverage or excluding coverage[4].

International Underwriting Association Cyber Endorsement

To help insurers comply with the Lloyd's mandate, the International Underwriting Association (IUA) surveyed insurers on their views as to whether PI policies ought to respond when a cyber event takes place. Based on the survey results, the IUA prepared a model clause[5].

Unfortunately, the IUA clause was not designed to be used in policies for regulated professions, which are subject to minimum terms and conditions (MTC). The Solicitors Regulation Authority (SRA) has confirmed that it would not expect insurers to add exclusions to the qualifying PI policy that could potentially conflict with the MTCs, and that the MTCs would prevail in such event. Helpfully, given the tension between the requirements of the Lloyd's mandate and the MTCs, Lloyd's has now granted a temporary dispensation from the requirements of the mandate until 1 October 2021 for the qualifying layer of insurance.

Despite the above, some insurers continue to endorse qualifying policies with a limited "Computer Breach" clause (with which Marsh has no concerns, as the exclusions are targeted only against first-party losses). However, as the Lloyd's dispensation does not apply to non-qualifying layers of insurance, we routinely see the IUA clause applied where excess layers are purchased.

1| There was a 337% rise in phishing scams in the first two months of the first national lockdown, National Cyber Security Centre, Weekly Threat Report 21st August 2020.

2| Supervisory Statement 4/17 'Cyber insurance underwriting risk.

3| https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/letter/2019/cyber-underwriting-risk-follow-up-survey-results

4| Lloyd's bulletin Y5277

5| IUA 04 017

The IUA Clause Applied to Theft and Ransomware

Theft of client monies

Under the Solicitors Accounts Rules, law firms are under a professional obligation to safeguard client funds they hold. Typically, they would expect their PI policy to step in if there were a theft of such funds.

The IUA clause excludes any liability for losses "directly caused by, directly resulting from or directly arising out of Cyber Acts". "Cyber Acts" are defined as unauthorised, malicious, or criminal acts.

Therefore, if a firm's systems are breached and funds stolen, without any act of the insured to assist the loss, the ensuing claim would be excluded as the loss is a "direct" result of the Cyber Act.

If, however, the scenario is one in which a fraudster purports to be, for example, a party to a transaction and emails the firm requesting the transfer of funds to a fake account, the exclusion would not be invoked. The employee's transfer of the funds is an "intervening step" in the Cyber Act, such that the loss is "indirect". As a result, the loss would not be excluded by the clause.

Ransomware Event

Where a firm is locked out of their systems until a ransom is paid, the firm's payment of the ransom monies would be a "direct" loss and so would be excluded by the IUA clause.

However, a third-party claim that arises as a result of the firm being unable to carry out its professional services while locked out of its systems, would be covered as an "indirect" loss.

Caveat Emptor!

The PRA and Lloyd's interventions have shaken up cover under PI policies for matters relating to cyber events.

If a firm holds client monies in excess of the limit of indemnity of their primary layer of insurance, its systems are breached, and monies above the primary limit are stolen, there is now a real risk that there will be no cover for those funds. This is especially worrying given that £3 million is the minimum level of primary layer cover mandated by the SRA for limited liability partnerships, and many firms would hold more than that, for example, monies held for completions on a Friday.

The use of third-party managed accounts (TPMAs), was featured in our August 2020 Risk Dimensions newsletter (https://www.marsh.com/uk/insights/research/risk-dimensions-december-2020.html). Subject to the terms, we believe such arrangements could be used to reduce or transfer some of this risk. However, TPMAs come with other associated risks, so careful consideration is required.

Conclusion

There is no "magic wand" solution to this issue. As such, our concluding message is "buyer beware" of what your PI policy covers, especially in the excess layers – unfortunately, it might not respond how you would have previously expected.

As things stand, Marsh is looking to develop solutions, but there is no current insurance option for this risk, and to our knowledge, market appetite to develop new approaches is not high.

For more information, or if you have questions about issues raised in this article, please contact your usual Marsh advisor.

We hope you enjoyed this edition. Currently our Risk and Error Management team is working closely with various clients to support their risk management efforts. If you would like to hear more about our service please get in touch with your normal Marsh JLT Specialty contact, or contact our team directly:

VICTORIA PRESCOTT
Risk and Error Management, Professional Liability,
FINPRO UK, Marsh JLT Specialty
+44 (0)739 212 3466
victoria.prescott@marsh.com

JOHN KUNZLER
Risk and Error Management, Professional Liability,
FINPRO UK, Marsh JLT Specialty
+44 (0)779 568 5584
john.kunzler@marsh.com

Insurance Brokers
Chartered