COVID-19 and Law firms: Managing the new and the old risks
April 2020

In the understandable focus on looking after people, managing cashflow and operating remotely, risk management has so far not been high on the agenda in the COVID- 19 pandemic. It should be.

Knowing your risks

Risk management is all about *knowledge management* – if you do not know your risks you cannot manage them. In this crisis which has caused law firms to operate in unprecedented ways, their risks are multiplied and intensified. With home-working the norm for the immediate future, is your firm aware of all its increased risks? How is it balancing the need for increased mobility with security of the organisation?

Law firms have even before this COVID-19 pandemic been identified by the UK National Cyber Security Centre (NCSC - part of GCHQ) as a major area of risk- and with every lawyer and business services person now working at home, this risk has intensified.

The fraudsters are already looking to take advantage of the disruption and use of digital networks and law firm management need to redouble efforts here to avoid loss. This covers not only ensuring that the cyber defences are fit for purpose but also that the main entry point for fraudsters- **your people**- are fully trained and operating with heightened consciousness of potential scams. The UK National Cyber Security Centre (NCSC, part of GCHQ) and US security agencies have now taken the unusual step of issuing a joint threat update on COVID 19 on 8/4/2020.

To quote the report "cyber criminals are targeting individuals, small and medium businesses and large organisations with COVID-19 related scams and phishing emails" (https://www.ncsc.gov.uk/news/security-agencies-issue-covid-19-cyber-threat-update) . As the NCSC reported in an earlier report. "There are several factors that make law firms an attractive target for cyber-attack – they hold sensitive client information, handle significant funds and are a key enabler in commercial and business transactions….. The primary threat to the UK legal sector stems from cyber criminals with a financial motive. However, nation states are likely to play an increasingly significant role in cyber-attacks at a global level, to gain strategic and economic advantage. There has also been some growth in the hacktivist community targeting law firms to achieve political, economic or ideological ends".

Law firms are required by the SRA to 'identify, monitor and manage all material risks to [their] businesses' – (para 2.5 Code of Conduct for Firms).

Given these current increased risks to law firms, the key question is how do law firms know that they have sufficiently robust systems, controls, policies, procedures and training in place to manage their risks and ensure compliance?

For example:

Supply chain analysis- out-sourcing key areas such as IT needs to be reviewed. Are they a source of cyber-attack, and what will you do if key parts of your supply chain become insolvent?
Physical security- offices are now largely empty- can they be accessed by fraudsters looking to obtain confidential data?

Only an audit from appropriate experts (beginning with looking at their IT systems and how they are currently being used) will identify where action is required and make recommendations as to the processes which will need to be followed to ensure compliance.

Training for your people

The people side is the first area to focus on. Phishing activities are significantly up and they will target people to click on links (NHS, COVID update etc.) that could give the fraudsters access to your systems.

Some of your people will be stressed and have money or redundancy worries – and this may make them vulnerable to cyber-crime approaches. It is noticeable already that business services / non fee earners are currently in the forefront of salary reduction and furlough and may be feeling especially vulnerable.

Secondly, is your client and firm data still safe? Are your people accessing data on personal devices which are vulnerable (and potentially beyond the firm's firewall)? Is your network now compromised? The reputational and financial risk of client data being compromised – and of course SRA subsequent action- is clearly a major issue.

In the current homeworking scenario, the need for mandatory training of your people to understand the risks to your firm from homeworking and the operating procedures to take so they operate safely should be provided urgently (and of course remotely!). Educating your people on changes to the technology landscape and an increasing focus on risk management and security should be a priority. Use downtime to your advantage.

Training does not just make good business sense to protect you, it is also a compliance requirement:

4.3 SRA Code of Conduct for Firms requires you to ensure that your partners and staff are competent to carry out their roles and keep their professional knowledge and skills up to date. Continuing competence goes far beyond 'black letter law', and the SRA say that **failure to take adequate steps to maintain competence may be an aggravating factor in disciplinary proceedings.**

Monitoring and supervision

Supervision and quality of output is always key – and of course can lead to complaints and negligence claims from the client. Supervision is not only a prudent action to manage risks but also a regulatory requirement – 4.4 SRA Code of Conduct for Firms requires firms to have an effective system for supervising clients' matters. How are you supervising the output of your lawyers and ensuring that you are continuing to deliver the quality that your clients expect?

This supervision also includes anti money laundering, where the SRA have been increasingly active and can result in significant firm or personal fines. Criminals are likely to target law firms where revenue pressure is highest, and vigilance should be high.

This is in addition to the usual risks identified by professional service firms- for example. Business Email Compromise (BEC) also referred to as a 'Man in the email' or 'Man in the middle' attack. This is a specific form of phishing where cyber criminals spoof the email addresses of an organization's executive (most of the times Managing Partner, CEO or Finance Director-level) to defraud the organization's clients and partners.

Cyber criminals can spoof the email address of an organization's executive to increase the credibility of an email. The attack is usually targeted at specific individuals in order to obtain money or confidential information. The methods usually used are electronic bank transfers. There are proven defences against this approach- for example using DMARC (Domain-based Message Authentication, Reporting and Conformance) is an email authentication protocol- but to date, too few law firms outside the largest firms are deploying them.

In addition, we are also seeing partners worried about strategic risk to their firms and themselves. A smaller firm has many advantages- control, genuine partner leadership, care for people and culture. However, a smaller firm can also be more fragile to market shocks than a larger firm. This can also be precipitated by partner retirement – whether planned or forced by ill health and subsequent capital issues.

These risk areas need continuous **monitoring** to review the effectiveness of your procedures in the new norm of homeworking. In addition to supervision, law firms need to now ensure they continue to carry out file reviews and encourage reporting of risk issues, and **positive self-certification** by every lawyer as to their compliance with procedures is likely to be an even better way to monitor behaviour during homeworking.

Managing risk in the new norm of homeworking is likely to require:

- Top level buy-in. Management must not only drive risk management but also live it
- Investment in training and education programmes to build awareness and change mindsets
- Continuous and systematic monitoring and reporting so managing risk becomes accepted as 'the norm'; and
- Adopting a zero-tolerance approach, as in *just do it!* Risk management in law firms can never be a voluntary matter in today's new world.

Financial stability

Unfortunately, it is likely that some law firms will have financial difficulties as a result of this crisis and the SRA Code of conduct for Firms at 2.5 requires them to monitor financial stability and business viability. If a firm thinks there is any risk of failure, then it should take appropriate advice at the earliest possible opportunity.

Where a firm gets into difficulties we have seen significant personal partner losses, especially if the partner has either retired or left the firm and the capital has not been repaid when the firm goes into administration or pre-pack. This can even endanger the family house where the partner loan is secured on these assets. For some firms, this additional risk may lead partners to conclude that it is less risky to be part of a larger firm.

We are strongly recommending that firms review their current risk in the new normal of COVID-19 distributed working. This will also enable the opportunities of new business models to be run with the new and the old risks properly managed and allow firms to survive and thrive safely.

If you would like to talk to us to discuss further, please contact Peter Scott or Paul Browne.