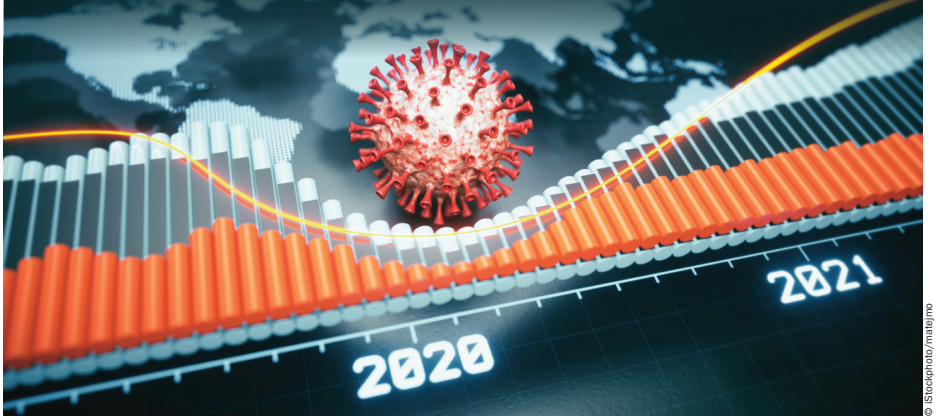
A sting in the tail?

Risk & compliance: Frank Maher provides expert analysis on the challenges ahead



© iStockphoto/matejmo

Law firms face an abundance of challenges maintaining financial stability and client service in a virus-ridden world—not just coronavirus, but the electronic sort too. There are also many detailed Brexit-related changes affecting even domestic firms. Here are a few areas to address.

Cyber—with a sting in the tail

A cyber incident may cause reputational damage which imperils a law firm's existence. This is not just an issue for large firms—hackers released personal injury client documents held by a US law firm.

According to the SRA Risk Outlook 2020/2021, in the first half of 2020 law firms reported losses of nearly £2.5m, and that there was a 337% rise in phishing scams in the first two months of the first national lockdown. The SRA published a thematic review in September 2020.

At present, client money—but not the firm's own—is broadly protected against cyber risks due to the extensive cover afforded under the SRA Minimum Terms and Conditions of Professional Indemnity Insurance (MTC), though no one wants a claim on their policy if it can be avoided. Conveyancing firms have been having a tough time with renewals as it is.

Increasingly, professional indemnity insurers' proposal forms have been asking whether firms have separate cyber cover, which will generally apply to the firm's own losses. The most important aspect of cyber cover is the assistance and support in the event of an attack —think of it like RAC or AA emergency roadside assistance; it may also cover other costs such as replacement IT and increased costs of working.

Of practical concern for readers is that professional indemnity insurers, in response to pressure from their own regulators, are seeking to limit the scope of MTC cover for cyber exposure. That will in turn make cyber policies more important, but there is a large caveat, because they may be subject to many forms of exclusion which are not permitted in the MTC.

Such exclusions could cause uninsured exposure retrospectively, because the product of an attack may be dormant on the firm's systems prior to inception of the cyber policy.

Hacking and ransomware are not the only cyber risks. We have advised on regulatory aspects in many cases where firms have sent emails to the wrong person. Specialist software using artificial intelligence can help prevent errors, and a short delay on outgoing emails may also be useful.

For all these reasons, and more, firms need to up their game on cyber protection. A starting point is the government's Cyber Essentials—preferably Cyber Essentials Plus—which is subject to external audit. Consider investing in advice from specialist external IT security specialists (who may not be your usual IT service provider).

Anti-money laundering & financial sanctions

This is another key risk area highlighted in the SRA Risk Outlook. They are still inspecting firms remotely. Issues raised include the requirement (where applicable) for screening, firmwide risk assessments (including evidence of the process by which they were produced), matter risk assessments, and treatment of Politically Exposed Persons (PEPs) and other higher risk clients and matters. Independent audit under reg 21 of The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (SI 2017/692) has been raised as an action item even with a provincial practice with fewer than ten partners.

Regulatory developments here include the requirement for firms doing any form of tax advice to have registered with the SRA by 10 January 2021; the requirement is wide enough to capture most firms as it includes providing assistance and material aid. Many are thought to have missed the deadline.

Brexit has resulted in some developments. Under reg 3 of the Money Laundering and Transfer of Funds (Information) (Amendment) (EU Exit) Regulations 2019 (SI 2019/253), the definition of a 'third country' is a country outside the UK, whereas it was previously one outside the EEA. This may affect compliance with the requirements for enhanced due diligence under reg 33 of the 2017 Regulations.

Revised guidance from the Legal Sector Affinity Group (LSAG) is expected imminently and it is expected to be published in advance of obtaining HM Treasury approval.

The UK is no longer implementing EU sanctions. All sanctions regimes will now be implemented through UK regulations. See the Office of Financial Sanctions Implementation website: *http://bit.ly/UKSanctions*. This is potentially an issue for all firms, not just large international practices.

Data protection

In another Brexit change, the new UK GDPR now applies. Firms will need to review their privacy notices and terms, though any changes are likely to be minor. Most firms use cloud services which give rise to consideration of international data flows. The Information Commissioner's Office has updated its guidance on international transfers: see *http://bit.ly/UKGDPR*.

International firms will have more to consider, and a decision is awaited from the European Commission on the revised draft Standard Contractual Terms. Transfers to countries such as the US are affected by specific issues though there may be solutions of which space does not permit further discussion.

Summary

Risk management and compliance are a culture, not an event. As the examples above show, the requirements are constantly developing and even for small domestic firms, they can be influenced by events on the world stage. NLJ

Frank Maher is a partner in Legal Risk LLP, solicitors, specialising in advice on professional regulation and professional indemnity insurance to professional firms. Resources on the above topics can be found at *www.legalrisk.co.uk*.