TheJournal
of THE LAW SOCIETY OF SCOTLAND

ARTICLE

Cyber risk - are you covered?

13 APRIL 15

Many businesses have been found to have a false belief that they are insured against harmful behaviour online - what about yours?

by Paul Motion

Attacks on a business carried out remotely by computer, or by fraudsters using a combination of IT systems and human deception, are unpleasant, stressful crisis events even for large businesses. For SMEs, and that includes most Scottish legal practices, the evaporation of a six-figure sum in a matter of seconds can threaten the viability of the business.

In addition to the immediate damage in terms of funds stolen, other consequences include business interruption or system downtime, significant non-chargeable time spent by management and staff, and possible reputational damage which can affect client or investor confidence in a business. A security survey produced in 2014 suggested that the average cost of remedying a serious security breach for large firms was between £600,000 and £1.15 million, and even for small firms the amount was between £65,000 and £115,000.

To the criminal threats can be added the existing power of the UK Information Commissioner to fine any business up to £500,000 for a serious personal data breach (or for spam e-marketing). That level of fine is about to be dwarfed relative to data protection by the General Data Protection Regulation currently completing its passage through the European legislature, whereby the maximum data breach fine is set to become €100,000,000 in 2017.

Boardroom myths

It is possible to insure against so called "cyber risks", by purchasing "cyber cover". In the author's view, this is a dated and unfortunate nomenclature, redolent of science fiction and mystique. It is more accurate to speak of systems breach and data loss cover. The "cyber" tag has possibly played a part in ensuring that hitherto, this issue has not featured high up the majority of boardroom agendas, and particularly so with SMEs.

Proof of this can be found in a recent report. Marsh discovered that 52% of CEOs believed their business already had "cyber cover" when it did not. The true figure was only 10%, and even that statistic could only be attained by combining standalone cyber policies (around 2% of market penetration) with such cyber cover as could be found scattered elsewhere in other policies. In relation to SMEs, i.e. the category into which most Scottish law practices fit, Marsh found the takeup of standalone cyber cover to be almost non-existent. The report disclosed that 98% of large UK firms lacked insurance that could help them recover from a serious cyber-attack. Remarkably, this was so even though 81% of those firms had also suffered a security breach in the last 12 months.

This low takeup is the more surprising, given the efforts which the EU and the UK Government have made to raise awareness of cyber risk. The EU Cyber Crime Directive 2013/40/EU EU Cyber Crime Directive 2013/40/EU states: "Cooperation between public authorities on the one hand, and the private sector and civil society on the other, is of great importance in preventing and combating attacks against information systems... particular attention should be paid to raising the awareness of innovative small and medium-sized enterprises to threats relating to such attacks and their vulnerability to such attacks, due to their increased dependence on the proper functioning and availability of information systems and often limited resources for information security".

Awareness agenda

In June 2014, the UK Government launched the "Cyber Essentials" scheme. This sets out the basic technical controls that all organisations should put in place to mitigate the risk from common internet-based threats. The scheme also provides a qualification, which demonstrates to clients, customers, tendering organisations and investors that the business has an awareness of cyber risk and has actively addressed the risk.

Insurers need to play their part in raising awareness, by doing more to explain the value to a business of cyber cover and setting out the role of such cover in combating cyber risk. The nature of the risk and extent of cover both need to be clear. As argued above, the regulatory penalty following a data breach may cause as much financial pain as the breach itself. There is a tendency for corporate boards to focus on technology, security and disaster recovery planning, rather than on evaluating organisational and information loss risks. Lloyd's, the Association of British Insurers and the Government have agreed to develop a guide to cyber insurance and to host it on their websites.

Overall the time is right for cyber risk to step out of the shadows and up the boardroom table.

Paul Motion is a partner with bto solicitors, Edinburgh