Hacked off with cyber risk?

You may be …

At the time of writing, news arrived that car owners in the US have filed a federal class-action lawsuit against Fiat Chrysler and a dashboard computer manufacturer after hackers used a laptop computer to take control of a Jeep being driven on a St. Louis highway, thus also precipitating a product recall and illustrating why Cyber risk is widely considered to be the fastest growing threat to businesses. A leading global insurer reports that it presents the "*biggest, most systemic risk*" faced by the market in over 40 years. Law firms are not immune.

This article looks at measures to guard against attack and its consequences.

Cyber breaches are proactive attempts to access, review and/or remove swathes of (often) sensitive information and, in doing so, disrupt the host firm(s). Law firms' possession of such commercially-important information and significant volumes of client data, renders them prime targets for hackers.

What risks are faced?

Increasing regulation, client confidentiality obligations and data protection requirements have thrust upon law firms obligations to protect information held within their 'virtual' walls. Despite over 75% of senior staff in the largest law firms believing that their firm will suffer from cyber attack, only 10% believe firms are ready to react effectively.

US evidence indicates that firms are already the targets of large scale *phishing* attacks. One such firm operated in ignorance of the theft of its entire client file database. Paperless offices lead to increased volumes of electronically stored documents and information (including personal, private, confidential and sensitive data) which become susceptible to attack.

Multinational companies, with their cross-jurisdictional operations and detailed acquisition plans, were initially targeted by hackers. Their IT security procedures consequently tightened, so the cyber criminals turned their attention to 'softer' targets – comprising the professional advisors who hold such transactional data.

Access can be gained in a variety of ways. The path of least resistance is created by users themselves, in particular where there is greater propensity for home-working. Rather than seek to break into servers via

sophisticated firewalls, hackers will target personal computers which possess only basic anti-virus software. Once access is gained, cyber attackers often hide in plain sight, monitoring the flow of information and gathering commercial intelligence. This places increasing numbers of clients at risk, not simply those in place at the time of the initial incursion, and puts the onus on firms to ensure that they monitor their own systems regularly and robustly.

What steps should firms take to counter the threat?

The starting point is to understand the risks faced. External sources will, inevitably, account for a large number of attacks, but law firms must also consider vulnerabilities amongst both staff and the devices and systems to which they have access.

First party and third party liability insurance are increasingly available to provide financial protection. In broad terms, the former will cover the loss of the firm's own data, and loss of business arising from a data breach or cyber attack. That cover will, likely, extend to loss of access to data arising from a network failure or denial of service and to the costs associated with corrupt, lost or stolen data. The cost of securing release of data held to ransom by hackers may also be included. Cover is available for the costs associated with determining the scope and extent of the breach and, from a reputational standpoint, the costs of providing early notice to those clients whose data has been compromised.

Third party cover will include potential liability to clients or imposed by regulators, arising from the loss of confidential information or data breach. The loss of client data could result in the loss of a high-value contract, the publication of trade secrets or wider reputational damage. The potential costs are significant. An insurance policy may also respond to a third party claim for losses caused by transfer of malware or virus, via the policyholder's systems, as the result of a hack.

As ever, cover will be subject to exclusions, so firms seeking cyber insurance should consider the consequent restrictions on claims. Potential exclusions will include breaches whilst the client data is in the possession of a third party (e.g. litigation support/expert) and the cost of replacing systems/hardware corrupted by a malicious attack.

To optimise premiums and cover, firms should endeavour to make themselves more attractive to Underwriters by demonstrating the extent of controls in place, the level of monitoring/testing of IT services and the extent to which portable media is captured within the firm's own IT framework.

Ultimately, the volume and sophistication of global hacking will make it difficult for firms entirely to block access to systems. However, firms have an opportunity, if they act now, to respond to the threats posed. Tightening IT infrastructure, and an informed purchase of insurance cover, will assist in fending off the challenges posed by this 21st century crime.

As a post-script, law firms should note the release of the domain *".law"* on 30 July 2015. Firms, if they have not done so, should consider securing rights to relevant domain names before cyber-squatters (who may cause reputational damage by establishing bogus sites and/or demand ransoms) do so.

Mark Aizlewood
Partner

T: 0203 697 1908
M: 07469 852355
E: mark.aizlewood@cpblaw.com

Simon Thomas
Partner

T: 0203 697 1909
M: 07469 856128
E: simon.thomas@cpblaw.com

"This information has been prepared by Carter Perry Bailey LLP as a general guide only and does not constitute advice on any specific matter. We recommend that you seek professional advice before taking action. No liability can be accepted by us for any action taken or not as a result of this information, Carter Perry Bailey LLP is a limited liability partnership registered in England and Wales, registered number OC344698 and is authorised and regulated by the Solicitors Regulation Authority. A list of members is available for inspection at the registered office 10 Lloyd's Avenue, London, EC3N 3AJ."