Cracking Cybercrime

Veronica Cowan explains why the failure to engage with cyber attack prevention is an unnecessary gamble

IN BRIEF

▶ Critical cyber-care and catching cyber culprits.

The Cyber Security Breaches Survey 2019, released by the Department for Digital, Culture, Media & Sport, found more businesses and charities are taking positive steps to improve their cyber security, partly because under the General Data Protection Regulation 2018 (GDPR) the Information Commissioner can fine firms which do not protect personal data. Nonetheless, cyber attacks pose a persistent threat, and recent attacks on law firms highlight their potential to cyber criminals, with smaller law firms often easy targets. According to the Solicitors Regulation Authority's (SRA's) 'Risk Outlook 2019–20', law firms lost £731,250 of client money to cybercrime in the first six months of 2019.

The SRA plans to conduct a thematic review next year into the impact of cybercrime on the legal sector, after data revealed at the Compliance Officers Conference in the autumn showed 23 law firms lost over £4m in the last year with insurers paying out over £3.6m to 16 law firms. The data showed some firms did not adequately record and report cyber-attacks, and a number had inadequate policies and controls. One firm failed to follow its own policy, and transferred £400,000 to fraudsters, and repaid the client from the office account. It recovered the money from its insurer, minus a £5,000 policy excess, but had to pay £900 compensation to the client who complained to the Legal Services Ombudsman.

Cracking cyber

The National Cyber Security Centre's (NCSC's) first report into the cyber threat to the UK legal sector published last year, reveals that 60% of law firms reported an information security incident in 2018—an increase of almost 20% from the previous 12 months ('The cyber threat to UK legal sector', see *bit.ly/2PbTZzJ*).

Ciaran Martin, its chief executive, notes that law firms are an attractive target for cyber attacks as they hold sensitive client information, handle significant funds, and are a key enabler in commercial and business transactions. The conveyancing sector is a well-known risk, but other areas are affected, too. Matt Webb, Hiscox's London markets cyber underwriter, notes law firms hold personal information—from tax, probate or personal injury claims, to M&A, patents or other corporate information—adding: 'Recent trends show increasing attacks on supply chains, and law firms are part of that chain for many companies.' The NCSC has launched the 'Legal Sector' group on the free Cyber Information Sharing Platform, a joint industry and government initiative set up to exchange cyber threat information in real time, in a secure, confidential and dynamic environment.

Cyber cover

As to cyber insurance cover, the Association of British Insurers (ABI) recently reported that take-up of this by businesses in the UK remains low, so how alert are lawyers to the risks? 'Law firms are exceptionally alive to the risks associated with cyber attacks and data breaches,' comments Jane Hunter, executive director and senior vice president of Aon. 'Brokers have also been raising cyber insurance policies with their law firm clients on a regular basis, identifying compelling reasons why it can be an important part of a firm's complete risk management strategy,' Hunter says, adding that finance departments, whose staff have to be alive to impersonation of senior partners in emailed requests for the likes of payments, bank transfers and false invoices, are particularly vulnerable.

Critical cyber care

But are law firms really switched on when it comes to diagnosing and curing cyber risk at their firm, given that research of 100 law firms revealed that 82% didn't even have the government recommended Cyber Essentials Accreditation. Chris Harris, CEO of the Practical Vision Network, highlights a mis-perception that only conveyancers are affected is one of the problems: 'Where organisations are targeted with malware and ransomware attacks …the whole firm is affected. One of the biggest growth areas is funds transfer fraud; where criminal organisations infiltrate matters to redirect remittance funds [including] probate funds, personal injury awards, divorce awards, as well as conveyancing funds. The failure to engage with cyber attack prevention is a massive gamble. Cyber criminals know the legal sector is underprepared.'

Legal practices have mandatory levels of professional indemnity insurance, but how about some of the business consequences of cyber attacks? Jennifer Millar, managing director, Aon, comments: 'We would expect all law firms to be insured for cyber risks to the extent that they cause losses to clients, and for this cover to be included in their professional indemnity policy. Other associated losses, such as regulatory investigations, breach mitigation, such as forensic and public relations advice and breach response, as well as the costs associated with business interruption would more typically be covered through a separate cyber policy.'

The ABI has cited the inability to access raw breach data risks as limiting the potential of the cyber market to price risk more accurately and manage exposure more effectively. According to Harris, professional indemnity insurers have identified cybercrime as a key area of risk for law firms and demand that they scope out their policies and procedures with regard to cyber mitigation, accounting for preparedness in their premiums. He adds: 'Law firms who fall victim to cybercrime are paying for it. Not only does it have a serious impact on clients' lives and well-being, but one study found breaches cost the average business £4,180, rising to £22,700 for larger firms.'

Millar says large law firms are insuring against cyber risks, adding: 'For the smaller firms, the percentage is much lower and this may be because they view coverage for their own first party losses to be a discretionary purchase.' Yet, small firms are common targets, partly because they don't have the necessary protections and systems in place.

Security of all data is important to a firm and its clients, given the consequences of its exposure to the wrong party, including the damaging effect on a law firm's reputation, Hunter observes, adding that certain data might be regarded as being particularly sensitive, including unregistered intellectual property rights, pre-listings information, merger and acquisition data, client contact lists and personal information about staff, or clients.

Cyber criminal culprits

The monitoring eyes and ears shouldn't perceive all the threats as emanating from outside the firm, because risks related to individuals represent the largest source of data breach claims. 'Cyber attacks often emanate from a disgruntled or resentful employee or ex-employee, so monitoring unusual behaviour can be vitally important,' warns Hunter. NLJ

Veronica Cowan is a barrister.