Solicitors Regulation Authority

News release

Greater than ever need for law firms to remain cybersecure

02 September 2020

With Covid-19 meaning huge numbers are now working remotely and carrying out both personal and business affairs online, a new report has highlighted the need for law firms to remain extra vigilant over the threat posed by cybercriminals.

Our Cybercrime Thematic Review takes an in-depth look at 40 incidents of cybercrime reported by law firms to us over a three-year period. While not all resulted in financial loss, the cases reviewed did collectively see more than £4million stolen by criminals. These figures do not include the wider impact and costs the crimes had on both law firms and their clients.

The review, which considered incidents that occurred between 2016 and 2019, found that law firms and legal transactions were still a common target for cybercriminals. Two of the larger firms visited reported that they were targeted by hundreds of different cyberattacks every year.

Most of the firms visited said they were aware of the dangers posed by cybercrime and felt that the most important factor in defending against it was the knowledge and behaviours of their staff. Despite this, we still found that only around two-thirds of staff in the firms we visited claimed to be 'knowledgeable' about cybersecurity and IT issues, with some senior figures even unable to answer basic questions about terminology.

Although human error was identified as their biggest risk, more than a quarter of firms visited did not have adequate cybersecurity policies and controls in place, while a fifth did not provide specific training on IT and cybersecurity.

Paul Philip, SRA Chief Executive, said: "It will be some time before the implications of the Covid-19 pandemic for the legal sector are fully understood, but we all know that millions more people than ever before are working from home, be they law firm employees or clients. That means the need for everyone to remain cybercrime vigilant has never been higher. Law firms should make sure that they have effective cyber security policies in place, and, crucially, that everyone in the firm understands and follows these day-to-day."

Good practice identified during the visits included the widespread use of anti-virus software, two-factor authentication for many sensitive

interactions, regular backing up of data, and nearly a third of firms holding specific cybercrime insurance.

However common incidences of worrying practice included:

- More than half of firms allowed external USB sticks to be plugged into company devices
- Two firms were using out-of-date Windows operating systems, with a further 16 using systems soon to become unsupported
- Firms did not necessarily report/know when they had to report incidences of data theft to the Information Commissioner's Office

In April we published dedicated Covid-19-themed cyber security advice [https://www.sra.org.uk/link/76b86126a3b549138a517f6ab86f5b3c.aspx] and Q&As.

The thematic review, published today, can be found here: Go to the thematic review [https://guidance.sra.org.uk/sra/how-we-work/archive/reports/cyber-security/]