Solicitors Regulation Authority

News release

Reports on cybercrime and innovation set out the risks

01 June 2022

- Four out of five cybercrime reports to SRA involve email
- Shift in ransomware attacks shows law firms' sensitive data at risk
- Innovation offers opportunity and risk, with almost half of legal services delivered online in the pandemic

A new report shows that email remains a significant vulnerability for law firms, involved in more than four out of five of all reported cybercrime incidents.

The information is in the SRA's new Risk Outlook report [https://guidance.sra.org.uk/sra/research-publications/risk-outlook-report-information-security-cybercrime/] outlining new threats as criminals look to exploit new technology. It shows that 83 per cent of cybercrimes reported in 2021 involved email – for instance, through email phishing attacks. Conveyancing has been the most common target for such attacks, but we are now seeing cybercriminals targeting a wider range of practice areas.

The report warns about the changing risks of ransomware. In 2021, we received relatively few – 18 – reports of ransomware attacks. Traditionally ransomware simply encrypted data meaning attacks would not have involved a breach to report. Newer ransomware steals data as well as encrypting it, with criminals likely to pressure targets by threatening to release sensitive information. We are now receiving reports from law firms of this.

Most ransomware attacks will likely be random, but they can be targeted. At a time of international tensions, firms acting for clients operating nationally significant infrastructure could be at higher risk, as could firms acting for Ukrainian, Russian or Belarussian clients.

It predicts that cybercriminals, aware that firms are focusing on the security of their IT systems, might make greater use of false physical documents or newly emerging scams where criminals carry out focused attacks using voice-modification software in calls to impersonate a solicitor.

Increasing use of the cloud and third-party IT systems also has risks. Although such providers are likely to have strong defences, the report highlights examples where attacks on them have led to malware being spread through firms' customers and multiple law firms.

Paul Philip, SRA Chief Executive said: 'Law firms are targeted by cybercriminals as they often hold large amounts of client money and/or sensitive information. It is in everyone's interest that firms take all reasonable steps to protect themselves and their clients, all the more so as innovation and increased use of IT make information security a priority.

'Protection isn't just about software. Having the right systems in place, such as anti-virus software or multi-factor identification, really matters. But good training and a culture in relation to managing risks is just as important.'

The report provides advice on steps firms can take to protect themselves, including training staff of information security issues in the office and at home, having multiple back-ups, and having a no-blame culture which encourages early reporting if something goes wrong. Firms that fail to assess their risks on a regular basis are vulnerable, as set out in our thematic review of cybercrime [https://guidance.sra.org.uk/sra/news/press/2020-press-release-archive/cybercrime-thematic-review/] . Further advice is available on our cybercrime pages [https://guidance.sra.org.uk/solicitors/resources-archived/cybercrime/] .

Alongside the cybercrime update, we have also published a Risk Outlook report looking at technology and innovation [https://guidance.sra.org.uk/sra/research-publications/risk-outlook-paper-innovation-competitive-landscape/] , with IT security as the common theme.

With 44 per cent of legal services delivered online in the pandemic, the report highlights some of the opportunities technology can bring, including responding to changing consumer behaviours and deliver services more efficiently. The potential risks that firms need to consider include data protection, some clients being unable to use technology, and considerations around liability if things go wrong.

The report also looks at potential future changes in the market including the implications of the use of artificial intelligence, cryptocurrency, and changes in the labour market where 70 per cent of young people say they expect employers to invest in their digital skills.

We offer a range of support to firms who want to innovate through SRA Innovate [https://guidance.sra.org.uk/solicitors/resources-archived/sra-innovate/] . This support includes advice, resources, practical tips promoting partnership opportunities and opportunities to test and develop new innovations in 'safe' regulatory spaces.

We are also encouraging firms to share their experience on information security cybercrime and innovation in a survey [https://form.sra.org.uk/s3/Risk-Outlook-2022] to continue to build our understanding of these issues.