www.lawyerchecker.co.uk
0800 133 7127
victoria.cope@lawyerchecker.co.uk

SRA – Security and Cybercrime

So what does the SRA say about why this risk matters?

- Keeping the affairs and assets of clients confidential and secure is a well-established professional responsibility.
- Clients increasingly expect the convenience and speed that IT can provide.
- Managing the risk posed by cybercrime is a regulatory requirement both from the SRA and the Information Commissioners Office (ICO).
- A cyber-attack could damage a firm's reputation and put off potential clients.

Trends

- There has been a national increase in cybercrime across all sectors. The City of London Police Commissioner stated his belief (in April 2015) that cybercrime may now be "bigger than the drug trade".
- ICO figures state reported data breaches by solicitors and barristers were the fourth most frequent of any sector, ahead of charities and the housing sector and behind only local government, healthcare and education.

Factors behind the trends

- Attacks using 'ransomware' which encrypt data and demand payment for it to be released back to the firm.
- Using details gained from hacking the firm to impersonate a bank or client. Often referred to as a 'Friday afternoon' scam as it often targets conveyancing firms at times when they are likely to be holding significant amount of money.
- Using information gained from hacking to impersonate the firm to clients, for example, by modifying bank account details to steal money.

Controls

- The Professional Principles in the Legal Services Act 2007 include a duty to maintain client confidentiality.
- Solicitors should also note that fines can be imposed by the ICO for a serious breach of the Data Protection Act.
- The most effective contribution we can make is to highlight this risk and encourage firms to take sensible steps to manage it.