

# Cybercrime

28 December 2023

Cyberattacks make up 75 per cent of all reported crime in the UK. Law firms and their clients are an attractive target because transactions often involve large sums of money, and law firms control sensitive information on behalf of their clients.

Rule 4.2 of the Code of Conduct for individuals

[<https://www.sra.org.uk/solicitors/standards-regulations/code-conduct-solicitors/#rule-4>]

and Rule 5.1 of the Code of Conduct for firms

[<https://www.sra.org.uk/solicitors/standards-regulations/code-conduct-firms/#rule-5>] place an obligation on the profession to 'safeguard money and assets entrusted to you by clients and others'. Everyone should be alive to the threat of cybercrime, and all firms should take steps to eliminate or mitigate against this risk.

## *Cybercrime risks*

The impact on clients and firms of successful cybercrime attacks can be immense. People could lose their homes, while firms have been shut down having been tricked into paying money out to fraudsters.

Cybercrime has therefore been a priority risk of ours for some time. You can find out more about why this is in our Risk Outlook

[<https://www.sra.org.uk/sra/research-publications/risk-outlook-202122/>] and in more detail in our report on cybersecurity in the new normal

[<https://www.sra.org.uk/sra/research-publications/risk-outlook-report-information-security-cybercrime/>] .

## *Thematic Review*

We visited 40 firms that had been targeted in a cyberattack to learn about their experiences. Discover what we found in our review

[<https://www.sra.org.uk/sra/how-we-work/archive/reports/cyber-security/>] .

## *Practical cybercrime advice*

We regulate nearly 10,000 firms, from sole practitioners up to multi-national corporations.

There is no such thing as a one-size-fits-all model when managing cyber-risks. We therefore leave it up to them to decide how they protect themselves and their clients from the threat of cybercrime.

Their primary focus will be understanding the specific threats facing them and tailoring responses accordingly as these risks evolve. We do not dictate what specific steps they should take.

Advice is available via the National Cyber Security Council, the government's free Cyber Essentials, and also the Law Society. You can find that here:

- National Cyber Security Centre [<https://www.ncsc.gov.uk/>]
- Cyber Essentials [<https://www.cyberessentials.ncsc.gov.uk/advice/>]
- Law Society Cyber Security Guidance [<https://www.lawsociety.org.uk/support-services/practice-management/cybersecurity-and-scam-prevention/cybersecurity-guidance-and-advice/>]

We have also examined the experiences of those firms that were part of our thematic review [<https://www.sra.org.uk/sra/how-we-work/archive/reports/cyber-security/>] of cybercrime and identified both good practice and areas for improvement to develop a toolkit for developing defences [<https://www.sra.org.uk/solicitors/resources/cybercrime/cybersecurity-advice/>] .