AILF INSIGHTS · AI AND TECHNOLOGY

Cybersecurity for law firms: protecting clients from digital threats

Law firms are attractive targets for cyber attacks. A plain-English checklist for Indian firms on phishing, ransomware, payment fraud and incident response.

Criminals follow value, and law firms hold a great deal of it: deal information before it is public, litigation strategy, personal records and money in transit. Firms are often easier to breach than their clients. Size is no protection. Small firms are attacked precisely because they are less prepared.

The common threats

Phishing. E-mails that imitate a client, a court or a colleague to steal passwords or deliver malicious software.

Business e-mail compromise. A fraudster takes over or imitates an e-mail account and sends changed bank details for a payment.

Ransomware. Software that locks the firm's files and demands payment.

Lost or stolen devices.

Insider error or misuse.

Weak vendors. Access gained through a supplier's system.

Twelve basic controls

1 Multi-factor authentication on e-mail and all remote access.

2 Unique, strong passwords with a password manager.

3 Automatic updates on every device.

4 Encryption of laptops and phones.

5 Regular backups, kept offline or separate, and tested.

6 Reputable security software on all machines.

7 Access to files limited by role.

8 Firm-owned e-mail accounts for all client work.

9 Verification of any change in payment details by telephone, using a known number.

10 Prompt removal of access when someone leaves.

11 Security terms in contracts with vendors.

12 Regular training, including simulated phishing.

Payment fraud deserves its own rule

Never act on bank details received by e-mail alone. Call the client or counterparty on a number you already hold. Tell clients at the start of an engagement that the firm will never change its bank details by e-mail.

When something goes wrong

Have a written plan. It should say who leads, how systems are isolated, which experts are called, how and when clients are informed, what must be reported under the law, and how evidence is preserved. Practise it once a year.

Legal duties

Firms have professional duties of confidentiality and obligations under data protection and information technology law, including reporting of certain incidents. Take advice on what applies to the firm.

Insurance

Consider cyber insurance, and read what it covers and requires.

Culture

Most incidents begin with one click by one busy person. Encourage staff to report mistakes immediately and without fear. An hour's delay can decide whether an incident is contained.

The business case

Clients ask about security before they engage. A breach costs money, time and reputation that may never return. Good security is part of professional competence.

Association of Indian Law Firms · November 2026
Read online: https://indianlawfirmsassociation.com/cybersecurity-for-law-firms-india/

Keywords: cybersecurity law firms India, law firm data breach, phishing lawyers, ransomware legal sector
Published by the Association of Indian Law Firms. General information only; not legal advice.