Cybersecurity Guide for Law Firms

We compiled key statistics related to cybersecurity from the top industry reports over the past 2 years to see the cost of a breach, the profile of hackers, why they target law firms, the common methods they use, and what you can do now to prevent an attack.

1 The cost of an attack

What is the average impact to a firm after being hacked?

Between 2021-2022, IBM estimated the **average cost of a cybersecurity attack between $4.24M – $4.35M** (2021 IBM, 2022 IBM)

Firms that have their data compromised could also be sued for malpractice, costing firms monetary penalties, time, and resources to resolve those cases.

Note: Monetary penalties are just part of the overall impact of a breach, the loss of business and negative impact on your reputation is unquantifiable.

2 Who hacks?

We profiled some examples of people who hack.

State-sponsored organizations attack firms to obtain knowledge their government may want.

Groups of hacktivists like **"Anonymous"** steal information and take over accounts to advance a political agenda.

3 Why target law firms?

Law firms contain confidential information for high profile individuals, corporations, and government agencies.

Hackers target organizations with classified client information (such as law firms) and threaten to release that data to the public if they are not paid a ransom.

90% of law firms have five or fewer employees dedicated to information security (2021 ABA)

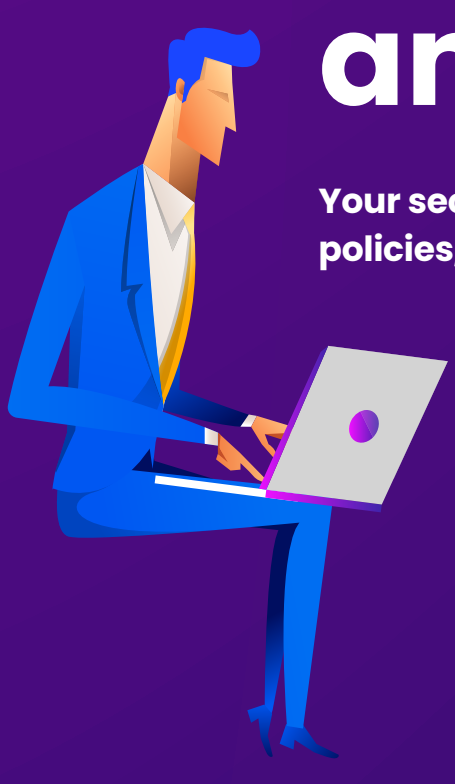
4 Common methods used by hackers

Hackers are constantly evolving how they attack your sensitive information and it takes a dedicated team to stay up-to-date with these new tactics to protect your firm and the clients you serve.

The **Bait and Switch** method uses things such as fake advertisements for real products and solutions to trick you into downloading malware.

Cookie theft is a way for hackers to view your browsing history, usernames, and passwords to steal other sensitive information.

5 What you can do now to prevent an attack



Your security policies should address: people, policies, procedures, and technology.

Stay up-to-date on the latest security software, use current versions of operating systems, promptly apply patches, backup your system, and train your staff.

Adopt **multi-factor authentication** that requires system users to provide two or more verification factors to gain access to your systems and data.

Aderant provides cloud-based solutions for your practice management, time capture, billing, and docketing needs. Our team of security experts work with the leading global cloud data protection companies to provide first-class security for your data.

This is just a preview of our researched findings. Click below to access our full analysis.

Access the full PDF