Law Firm Data Security: Challenges and Risk Management

January 18, 2022

Cybersecurity has emerged as an area of great importance for law firms. The potential exposure of sensitive data is a nightmare scenario for any law firm, no matter its size and scope of business. Unfortunately, it's easy to overlook law firm data security amid attorney's hectic schedules and deadlines.

Hackers have learned over time that a law firm's data security must protect vast amounts of sensitive information, including data protected under attorney-client privilege. Law firms are an ideal target for ransomware schemes, but the damages from cyberattacks go beyond catastrophic security breaches.

Damages incurred can include potential malpractice suits from clients and losses in reputation, time, and productivity. Some reports estimate that the financial damages from successful hacks average upwards of $1 million per attack.

The problem has become so prevalent that the American Bar Association (ABA) has set forth a set of guidelines for what attorneys are responsible for in the data security of their law firm. We'll delve into those guidelines later in this post. For now, we'll start by looking at the types of cybercrimes and risks faced by attorneys, the value of creating a cyber risk management plan, and how to get started.

Types of cyber risks

A data breach is defined as an instance when unauthorized users view sensitive data. While the term automatically conjures up images of hackers, simple security oversights such as a lost or stolen device are often the causes of data breaches. Nevertheless, accidental breaches are a reason to follow good data hygiene.

Hackers and cybercriminals use a few different types of malicious attacks. Some of the most common include:

- **Phishing scams**: Emails or social media messages designed to trick the recipient into revealing sensitive data.
- **Ransomware**: Viruses that lie dormant in a computer or mobile device, and once activated, create a layer of encryption that conceals internal data from the victim. The virus slows down or halts internal systems until the victim pays a ransom.
- **Spyware**: Viruses that steal sensitive data and send it back to the attacker, avoiding detection. They are a variation of ransomware.
- **Brute force attacks**: A program hacks into a computer or network by guessing credentials through trial

and error.

Also read:

4 Tips to Prepare for a Communication Association Cyberattack and Data Breach

Law firm data security obligations

In 2018, the American Bar Association established **guidelines for attorneys to follow** when handling law firm data security. ABA states that it's "not a matter of *if*, but *when*" attorneys and firms will experience a data breach. These guidelines give law firms a solid understanding of what to expect and what attorneys should do in the aftermath of an attack. The guidelines include:

- **Duty of Competence:** Law firms must take adequate security measures regarding technology.
- **Obligation to Monitor:** Lawyers must continuously monitor their systems and take steps to mitigate cybersecurity risks.
- **Stopping the Breach:** An attorney or firm must take all the proper steps to plug the breach.
- **Notice of Breach:** If public or client information was exposed from the data breach, the firm must give due notice to the exposed parties.

Practicing good cyber hygiene

While a data breach may be unavoidable, there are steps you can take to protect your firm and minimize the risk.

- Enforce secure passwords
- Use role-based authorization
- Implement multi-factor authentication
- Update software regularly
- Train employees in cybersecurity
- Encrypt data
- Conduct regular cybersecurity audits

Beyond basic cyber hygiene best practices, law firms also need to have a plan in place.

Read more:

What to Look for in a Lawyers Professional Liability Policy

The value of actively managing your law firm data security

It's only a matter of time before every law firm faces the threat of data breaches. Unfortunately, breaches still happen despite the best intentions and practicing good cyber hygiene. That's why all lawyers would benefit from devising a management plan for law firm data security and signing up for McGowan **Lawyers Professional Liability Insurance**.

In addition to cybersecurity coverage, McGowan's professional liability insurance includes:

- Wide range of coverage options, limits, and deductibles
- Pricing consideration for part-time and newly admitted attorneys
- Portfolio of complementary risk and claims management services
- Access to Loss Prevention Hotline (up to 4 hours no charge)
- Access to Risk management website
- Dedicated claims support staff available 24/7
- Subpoena assistance

Don't let the inevitable derail your law firm. **Contact McGowan insurance experts today** to learn more about the risk of cybercrime.

Like Tweet

SHARE THIS POST

PREVIOUS
Put Event Safety First With a Venue Risk Assessment

Search...

Privacy Policy