Published on *The National Law Review* https://natlawreview.com

5 Law Firm Cybersecurity Threats Solved with Legal Practice Management Software

Article By:

Bill4Time

With all of the sensitive and oftentimes personal data law firms store, it's no surprise that law firm cybersecurity threats are at an all-time high. No matter the area of practice, law firms maintain a wealth of vital client information, valuable intellectual property, sensitive business information, and other confidential or proprietary data. As the legal industry shifts to remote and hybrid work, cybersecurity has never been more of a concern for law firms. In 2020 alone, the American Bar Association discovered that 29% of surveyed law firms experienced some type of cyber attack, which is a 3% increase over 2019. Unfortunately, only 34% of those surveyed had developed an attack response plan.

Law Firm Cybersecurity Threats

Cybersecurity is evolving. It's no longer reserved for technology, but it's now one of the greatest risks a law firm can face. In recent years, massive law firms in the United States have been caught up in major cybersecurity breaches that cost millions. Cybersecurity is not just in the realm of the IT department, or for small firms, a risk that isn't worth addressing. It needs to be part of the general guidelines for using technology in the firm – or in its service.

Cybersecurity is a big undertaking and some firms are too small to have the full weight of IT professionals behind them. Medium and large firms may be delayed in preparing for cyber-attacks because of the costs, or they assume it won't happen to them.

Overall, law firms have been largely analog until recently. Lawyers and staff tracked client and firm information manually, limiting the risk of a cyber breach. Firms are getting on board with innovation, however, and clients are expecting more technologically advanced communications and approaches – meaning that law firms are now open to the risk of a cyberattack that wasn't present before.

1. Backing Up Critical Data

Data and IP are critical to law firm operations. Attackers often install malicious software to block access to computers or the data they contain, asking for a ransom to return the data (known as ransomware). This is a major concern for law firms since just one ransomware attack could render huge volumes of data inaccessible.

With regular backups, however, a ransomware attack isn't as critical. All vital data is copied and stored on an external hard drive or a secure location that's separate from the network, ensuring the information is still accessible and safe during a cyber attack. This also minimizes the downtime a law firm may experience from an attack.

2. Regular Updates and Patches

Cyber attackers are good at finding ways around cyber security defenses. Software and operating systems that haven't seen regular updates give cyberattackers ingress points to exploit vulnerabilities and gain widespread access to the system and data within it.

Software updates are usually performed to optimize performance or fix a bug, but they have the added benefit of shoring up cyber security. Patches are a bit different and are intended to address security vulnerabilities. These should always be applied as soon as they become available.

With legal management software through a provider, software updates and patches are applied as needed, keeping security in a law firm's network as ironclad as possible.

3. Access Control and Authentication

Strong, complex passwords are an excellent line of defense against a cyber attack. Passwords prevent full access to accounts and the sensitive information and data they contain about the business or clients.

Unfortunately, law firms often have integrations with services and systems like DocuSign, DropBox, and more. If just one of these systems is compromised, an attacker could gain access to a lot of valuable information.

Throughout the law firm, all staff members should have strong passwords that combine upper and lowercase letters, numbers, symbols, or phrases that are difficult to guess. When staff members rely on weak, easy-to-remember passwords, especially for multiple accounts, it's easier for attackers to see what other accounts they can access with just one password.

Tools like a password manager and multi-factor authentication add a layer of defense to ensure that only verified staff members have access to the system. This way, even if an attacker gains a password, they have to go through multi-factor authentication to have full control of the account.

Furthermore, legal practice management allows law firms to configure different users for different access. All functions can be configured with specific user permissions and customizable user access. Contractors can have temporary access, and law firms can track logins automatically to see if anyone is using their credentials inappropriately.

4. Virtual and Physical Protection

Data is not only vulnerable to attackers, but it may be vulnerable to external circumstances like natural disasters and local outages. When these occur, valuable data can be lost or vulnerable.

Legal management software has data centers that are geographically distributed to minimize the effects of regional disruptions. They also have redundant power systems and environmental controls

to provide 24/7 uninterrupted service. If service or upgrades are required, the law firm experiences minimal downtime or disruption.

5. Cybersecurity Expertise

Lawyers are good at practicing law, not at shoring up cyber security. It’s best for law firms to outsource cyber security protocols and procedures to experts, which can be achieved with legal practice management software.

Software providers work with trusted third-party leaders in data security to meet or exceed security standards, including putting forth policies and practices for world-class information security. This includes possible threats, how to respond to them, and weak points in devices like desktop computers, smartphones, laptops, removable data storage, security cameras, and more.

Legal Practice Management Software Can Limit Law Firm Cybersecurity Threats

Legal practice management software has many benefits for a law firm, but one of its biggest is that it helps with cyber security. Threats are everywhere and expanding as firms add more users and technology, but understanding the threats and implementing the right software solution can help law firms shore up their defenses.

National Law Review, Volume XII, Number 152