centerbase.com

Centerbase CloudBased Law Firm Management & Growth Platform

Your Guide to Preventing Law Firm Cyberattacks

developers · Tuesday, November 9th, 2021

In this digital age, technology has become essential to the delivery of legal services. Law firms use tech tools for a variety of reasons, including matter management, calendaring, client communications, and billing. While this reliance on technology has helped law firms improve client relations and the provision of services, it has also made the legal industry a common target for cybercriminals looking to steal valuable client data.

This increased risk has become all too apparent over the past few years, as several well-known law firms have been forced to deal with the disruptions of a cyberattack. The methods used by these criminals are becoming increasingly complex, which means that the frequency of law firm hacks will likely increase.

For this reason, law firm leaders and administrators must implement cybersecurity measures to fight this persistent threat. It is an ongoing battle that requires a consistent response.

Ransomware

Ransomware is often the weapon of choice for cybercriminals targeting law firms. With this type of hack, a third party takes control of a firm’s files by encrypting them and denying any access to firm members, unless a requested amount of ransom is paid.

A ransomware attack can leave an entire firm without the ability to work, which immediately decreases revenue. Additionally, the firm may face consequential damages, including:

- The cost of paying the high ransom demand
- Unsuccessful insurance company claims
- Negative press, which makes potential clients uncomfortable and unwilling to work with the firm
- Lawsuits (and related court costs) from clients affected by the breach

Phishing

Another common type of cyberattack against law firms involves an email phishing scam, where hackers pose as firm clients or third parties to trick employees into disclosing sensitive data or transferring funds to fraudulent organizations. Attorneys are particularly susceptible to email fraud attempts due to the personal relationships that may have with their clients. A spot-on impersonation may lower a target’s defenses, leading to significant losses.

In one infamous New York case, a law firm was successfully sued for malpractice by a client after

hackers impersonated one of the firm's attorneys to secure a fraudulent $2 million wire transfer. The attackers were able to gain access to the attorney's AOL email account and analyze previous interactions with the client to successfully carry out the impersonation.

As you likely gleaned from the above, the financial and professional consequences of both ransomware attacks and phishing scams can be detrimental to a law firm, so it is critical to take the necessary steps at your own firm to prevent such an occurrence.

Preventing a Law Firm Cyberattack

Preparation is the only adequate protection against a cyberattack. This starts with understanding the threat and the role that technology plays in reducing it. Attorneys have a duty to not only comprehend the practice law, but also the technology necessary to protect attorney-client privilege and sensitive client data. Most states specifically include this in their rules of ethics because the reluctance of attorneys to introduce technology tools into their law firms increases the chance for a breach.

By refusing to implement tech security measures, attorneys may be found in breach of their professional duty. In addition to ethical consequences, firms also face regulatory enforcement actions from the Federal Trade Commission when client data is not sufficiently protected.

However, there are steps that you can take to strengthen your firm's protection against security hacks:

Educate Firm Members

Cybercriminals capitalize on limited knowledge and bad habits. Law firms that ignore best practices and utilize weak security systems are essentially opening the door for attackers to access valuable data.

One of the most effective steps a law firm can take is consistently educating and training employees. Human error accounts for a significant number of cyberattacks on businesses. Training sessions should occur on a regular basis to educate employees about their role in preventing breaches. Regular reminders should also be a part of the training plan to ensure that these important duties remain top of mind.

When armed with the right tools, educated employees provide law firms with a strong first line of defense. By acting in a responsible manner, they help close gaps of vulnerability and provide your firm with greater protection.

Perform an Audit

A detailed audit identifies weaknesses before a breach can occur. The first step of an audit should include an inventory assessment to help your firm understand where you stand with respect to technology products utilized.

Technology consists of both hardware and software, as well as data. Hardware includes the maintenance of all computers, servers, laptops, and printers within the firm. Smart devices should also be included with hardware because they are often the vehicle through which attorney-client privilege is breached.

Taking inventory of software products involves a review of all licenses, keys, and passwords. Firms also need to make sure that all software is updated on a regular basis with the most recent versions. Outdated software is more likely to lack sufficient protection against continuously evolving cyberattack techniques.

Data inventory requires the consistent monitoring of what data is stored and how it is maintained. Law firms should consider designating a data administrator who regularly audits the firm's data for ethical and regulatory compliance.

The second layer of the audit involves answering numerous questions about the firm's security, such as:

- Are systems in place that limit access to credentialed parties only?
- Has encryption been implemented for all smart devices and computers utilized for firm-related business?
- Are password records strong and changed on a regular basis as a matter of firm policy?
- Are anti-virus software and firewalls in place?
- Does the firm have cybersecurity policies in place that have been regularly communicated with every firm member?
- Have intrusion detection and network security controls been installed across your entire network?
- Are file backups occurring on a regular basis to prevent loss of data should a breach occur?
- Have steps been taken to secure all firm workstations and endpoints?
- Is the firm operating in compliance with security best practices within the legal industry?

Answering these questions will give law firm leaders and administrators a clear view of where the firm stands with its technology and where it still needs to go.

The services of a security expert can be useful during an audit to ensure that firm networks adequately store firm data. If employing an expert is not an option, a security consultant can also be contracted to assist with the audit.

Establish a Security Plan and Budget

The bottom line: law firms need to craft a security plan and implement it. Basic tools, such as spam filters, anti-spyware, antivirus programs, and network security protocols should be implemented. But your responsibility does not end there.

Many law firms often neglect their first point of contact with the outside world, which is the firm website. When cyber attackers see an outdated website, they may target the law firm under the assumption that their inadequate security measures extend to the entire firm.

Document management is another important component of an effective cybersecurity plan. Law firms maintain countless documents and files that must be handled and stored correctly. A secure document management system prioritizes the protection of files while they are in storage, as well as during transmission. A comprehensive practice management system and email encryption are two tools that law firms can use for successful document management.

A reliable backup system must also be a part of a law firm's security plan. Cyberattacks can interrupt business in an irreversible way. A backup system helps you get back to work quicker, even in the wake of a disruptive ransomware attack.

Some law firms hire a security consultant that specializes in cybersecurity. Others contract an outside security expert to guide auditing, consulting, and implementation. Firms should include this necessary expense in their annual budgets. Firm leaders and administrators may also consider the cost of purchasing a cyber liability insurance policy for the firm.

Vendors should also be included in law firm security plans. Firms use third-party vendors for a variety of services and products, but they often take for granted that these providers are employing adequate security practices. Firms should review the security certificates of every vendor to ensure that their security protocols are up to par. Law firm vendors need an understanding of the unique importance of protecting law firm data. Their commitment to the protection of client data should match, or exceed, that of the law firm.

Law Firms Must Take Steps to Minimize Cyber Threats

When law firm leaders fail to plan, implement, and enforce strict cybersecurity protocols, they are potentially exposing the firm to costly and damaging attacks. Though it will take some time and money to get adequate plans in place, when done correctly, it is one of the best investments a firm can make to deter fraudsters and keep client data secure.

This entry was posted on Tuesday, November 9th, 2021 at 12:00 am and is filed under Compliance & Security
You can follow any responses to this entry through the Comments (RSS) feed. Both comments and pings are currently closed.