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

Cybersecurity Is More Important Than Ever for Law Firms

Article By:

Eddy Bermudez

Cybersecurity is one of the biggest issues of our time. With more data being stored online, and law firms managing increasing quantities of sensitive client data, the threat of hackers has never been greater. Without appropriate cybersecurity tools, even data you think is safe can be accessed by unauthorized users. For this reason, cybersecurity advancements are being made all the time.

Many law firms throughout the United States are yet to catch onto this important service, and there are many reasons why law firms should be concerned. With personal information, addressed, and confidential records being stored by lawyers online, hackers have more targets every day. For this reason, legal professionals should consider their Internet security.

Why Should Law Firms Invest in Cybersecurity?

According to a 2016 report by Symantec, the threat of email hacking and malware is growing. Between 2014 and 2015, the amount of new malware grew from 317 million to 431 million. Crypto-ransomware attacks rose from 269,000 to 362,000. Web attacks also grew in the same timeframe from 493,000 per day, to 1.1 million per day. This is a real and growing threat, and one that doesn't appear to be going away any time soon. Without proper protection, law firms face an uphill battle to keep sensitive information secret.

In 2015, this real and growing threat became evident. The legal world was rocked by the Panama Papers scandal, where 11.5 million documents that contained sensitive client information and financial records were leaked from Panama-based law firm Mossack Fonseca. The leaked files made personal financial records of wealthy people and elected public officials public, with offshore accounts

becoming a major focus for the press. Since then, it has been evident that the legal world faces a serious threat.

For any law firm, the leaking of information is a serious problem. With data being handled mostly through computer systems, hackers can obtain information that is legally protected. The effect of such a leak is wide-ranging, too.

Not only can law firms face legal action for allowing data to be released, but the reputation of the firm will quickly evaporate. Large companies will switch to firms with more thorough computer security, and some legal professionals may never recover from the scandal. All this can occur as a result of outdated software or a lack of encryption, In the Mossack Fonseca case, millions of files were obtained as a result of the company using out-of-date security software, and not encrypting their emails.

Five Ways a Law Firm Can Improve Client Data Protection

Improving your online practices protects both client data, and any sensitive business data relating to your firm. Here are four ways you can improve your law firm's online safety.

1. Use Password Managers

Password managers are secure ways to store username and password information. This is the best way to avoid the common practice of reusing the same password through numerous different systems. Using the same password significantly reduces your online safety, making it easier for hackers to access more of your personal and client data. Password managers make it easy to keep track of the passwords you use, and can minimize the damage caused if one account is hacked.

2. Update Computer Software

Updating operating systems and software on your computer is important. Software companies regularly provide updates and patches for holes in software that are vulnerable to hackers. When you update your software, you are patching any potential gaps in security, making it less likely that your information will be compromised.

This is particularly important for operating systems, whether you're using a Windows, Apple, or Android computer. Computer settings allow you to switch on automatic updates, which are typically installed overnight. The same is also true for smartphones, which prompt the user to update whenever a patch has been released.

If you use anti-virus software, the same rule applies. Anti-virus applications will provide regular updates about any potential malware that has been stopped and will also inform you when important updates should be downloaded and installed.

3. Use Encryption Software

Encryption software can be installed on computers as well as mobile devices. An encryption application will protect data even if somebody gains physical access to your device. Some cell phones even have encryption built in, along with a "wipe" feature that corrupts all personal data when the device has been reported stolen.

4. Use Online Encryption

When storing data in the cloud, encryption is essential. Legal management software like PracticePanther offers encryption for all data, with an integrated cloud storage system. All data stored online is encrypted and protected using HIPAA compliant technology.

5. Use Two-Step Authentication

Two-step authentication is one of the simplest ways to protect your data. Instead of just using a password, two-step authentication will require an extra step when logging into an unknown device. All major online systems provide this service, from Google and Facebook, to Microsoft and Apple. PracticePanther also provides two-step authentication on their online legal management system, which sends a security code to your email address if somebody tries to log into your account on an unknown device. This prevents unauthorized access and informs you when your password has been compromised.

Take Action Today

In 2017, this is an important step for every law firm to take.

National Law Review, Volume VII, Number 234