Law Firm Cyberattacks: Is your firm protected?

Law firm cyberattacks are more and more common. Could you live without your files for 3 months?

Cybercriminals used ransomware to attack a prominent Providence law firm. Every single one of their files became inaccessible after the criminals encrypted everything and denied access. This meant all ten attorneys at this firm were unable to work as the firm bled money they couldn’t afford to lose.

The losses were large, unnecessary, and growing. A few lines of code from a self-serving attacker created millions in losses:

- $700,000 in billings
- $25,000 in Bitcoin ransom
- Another ransom, because the first unlock code failed
- Court costs, expenses, and lawsuit fees against the firm’s insurance company who denied their claim for lost billings
- Negative press, which discourages prospective clients and kills any negotiations in-progress

- Lawsuits from angry clients whose legal needs were negatively impacted

How many clients did they lose to this whole affair? How many prospective clients determined that they would rather do business with a more secure and reputable firm?

Preparation is key to protect from a cyberattack

Matthew Perry's law firm was attacked by cybercriminals, twice. Both times, his firm survived unscathed. How were they able to protect their data and preserve their reputation when other law firms fail?

https://www.youtube.com/embed/zCMuHCYar-k"

Don't wait to prepare. If you haven't already, hire a security consultant that specializes in auditing cybersecurity. Then, hire a specialist to properly educate your team and set up your firm's network and security practices.

You need to do a security audit to ensure that your firm:

- Has cybersecurity policies in place to protect your firm's work product
- Has intrusion detection and network security controls across your entire network
- Runs antivirus with heuristic protection which enables you to identify new threats before they cause damage, without the need for a specific signature.
- Conducts regular file backups to preserve data in the event of a breach or downtime
- Regularly tests backups, following the schedule recommended by your security expert
- Uses multi-factor authentication to verify identity and protect from remote attacks
- Encrypts inactive data being stored on any device (data-at-rest) as well as data in motion (data-in-transit)
- Protects workstations/endpoints
- Ensures that software and hardware is regularly updated and compliant with security best practices

Luckily, there are programs that do a lot of this work for you. A cloud-based practice management software, like Bill4Time, performs automatic updates and backups your law firm's sensitive information regularly.

Train your team to avoid a cyberattack

Law firm cyberattacks are avoidable and starts with being proactive about closing gaps of vulnerability. Any gaps in your security can lead to severe financial and data loss.

Cybercriminals rely on bad habits and inexperience. They attack businesses with weak security and those not following best practices. As Matthew Perry has shown, it’s possible to meet these attacks head-on and win. You’re a highly trained legal professional — strong, capable and intelligent. This means you can solve this problem.

Don’t wait for an attack to find out you’re unprotected. Work with your security experts to make sure your network is secure, and all law firm data is safe. Trust but verify that the security protocols you are following are working to protect your firm.