6 Step Ransomware Defense Plan for Law Firms

Whether you've been listening to a colleague extoll the difficulties of Bitcoin transactions or you've fallen victim to an attack yourself, you're likely well aware that ransomware attacks are no longer just a problem for 'other businesses'. Law firms are directly in the crosshairs of cyber criminals for one simple reason – they make for a *great* target.

Why? First and foremost, law firms are still very late to the security game. American Bar Association (ABA) model rules of conduct are pushing awareness but the mindset of 'I'm not big enough to be a target' still lingers. This assumption couldn't be more wrong.

Here's why. The underlying principle of 'I won't be hacked' assumes that criminals are targeting law firm data so it can be used for nefarious intent. Think 'insider trading'. The simple truth is that they are targeting law firms with Ransomware because they have low security, have very sensitive data and will pay a lot of money to keep it.

So they simply breach your network, encrypt your information, pull the encryption key so files are unreadable and tell you to pay thousands to get the encryption key back. It's happening to law firms every day, but you can proactively fight, and help prevent the headache you will have to face after a malicious hack.

First, understand how ransomware attacks begin. Generally speaking, there are only **two ways** that critical systems can be attacked **– web based infection or an email based infection**.

The first means of attack – web – can originate from malicious advertising or a website that has been compromised all together. These websites can be work related (e.g., LexisNexis) that look and act exactly as the uninfected original site. Opening the page and clicking on a link initiates the ransomware payload / download.

The second means of attack – email – is very common and also very difficult to defend. Through social engineering, the sender (criminal) includes just enough personal information to get you to

click on a link or download an attachment. 'Your Refund' and 'Invoice Attached' are common social engineering tricks played on people with surprising success.

Knowing the way an attack is likely to occur means putting yourself in a good position to stop an attack early in the process. Avoiding a disruptive and money-losing ransomware attack can best be accomplished with the following 6 steps:

1. Leverage OpenDNS to control outside traffic. Many ransomware attacks leverage known IP addresses that, if blocked, can prevent ransomware payloads from ever being downloaded.
2. Employ spam filtering that validates attachments. Better solutions such as the Barracuda Essentials hosted spam filter will scan attachments and even test executables to ensure the file does not call to another criminal website for a ransomware payload/download.
3. Perform regular vulnerability testing and patching. Do not wait for your software or hardware vendors to fix holes in their systems. Rather, test your network at least once a month for vulnerabilities and immediately patch any issues found.
4. Disable Remote Desktop Protocol (RDP). Unless this is required, the feature should be turned off so that outside parties cannot gain control of a desktop within the network.
5. Train your team on how to spot malicious email. One simple rule to follow – if you did ASK to have something sent to you, call the sender and check to be sure the email is legitimate. If you have no way to contact the sender – delete immediately. Occasionally test your users with a social engineering tool such as KnowB4.
6. Extend your back up cycle. A weekly incremental backup with monthly full backup can work. However, do not delete the older month's back up. Keep at least six months of full back-ups both locally and off site, preferably in the cloud. Newer ransomware attacks are encrypting data much longer in order to encrypt the very backup you may need to recover your data. Datto and Barracuda both provide excellent solutions for this type of security backup.

Unfortunately there are no means to completely insulate yourself or your firm from an attack. But following these steps and working with your IT Management team to continually test and evaluate your defensive measures for efficacy is your best chance for success.