With so many high-profile cyber breaches and ransomware incidents in the news, it is easy to become overwhelmed. If large technology companies cannot keep out the hackers, how can we expect small to mid-sized law firms to do so?

The reality of many cyber breaches is that basic security controls could have prevented the incident from ever occurring. Even high-profile breaches that make the news could have seen better prevention and faster recovery by implementing industry best practices. For law firms, many breaches do not occur because cyber criminals have hacked through a firewall, they occur because of a failure to implement very standard security measures.

To reduce your Firm's risk of cyber breach, your firm MUST INSIST that your IT team implement these measures.

- Multi-Factor Authentication for ALL accounts (network, email, Document Management, banking, social media)
- Security Awareness Training from a company like Arctic Wolf or KnowBe4
- Cleanup of Old User Accounts
- Data encryption
- IP Filtering for Remote Access
- Security Awareness Training

As a 25+ year IT professional focused on the legal space, I have heard every reason for not making it more difficult for the attorneys to access the network.

> *There is not enough money in the budget to secure the network.*
>
> *The partners do not have the time or patience for more layers of security, and they certainly do not want to have to remember all of these passwords.*
>
> *Our firm is too small, and the data we keep on the network is not of value to hackers.*

Cyber criminals are successful because they can count on firms to lean on these excuses.

The reality is that most firms have already spent some of the money needed to implement these basic security measures. It also is not that expensive to implement the rest.

Here are simple measures your Firm could implement immediately:

- **Multi-Factor Authentication**. This is included with Microsoft 365. Your IT team just needs to set it up and train your users.

- **Strong passwords**: Many online services recommend or force users to set long and complicated passwords. Training users to follow those recommendations rather than selecting the easiest option to pass – like adding a symbol to their favorite password – will improve the firm's overall security.

- **Data encryption:** Cloud servers commonly allow you to encrypt the data stored on their cloud. Set a priority at your firm to learn the process and implement the practice.

- **IP Filtering:** This can be implemented by your IT team to filter out remote access attempts from outside of the United States (unless your Firm has partners outside of the US). IP filtering does not prevent people from outside the US from visiting your website or sending your firm email.
- There are many companies that include Security Awareness Training as part of their service.

- **Security Awareness Training:** Look into companies like Arctic Wolf, KnowBe4, and BullPhish. These companies will teach your team how to recognize suspicious phishing emails and dangerous links.

It has always been very easy for firms to find excuses not to implement basic security; however, these excuses will soon cost firms hefty bills in recovery. The legal industry's approach to cyber security needs to change; basic security is better than no security.

A thief does not always steal from the nicest car in the neighborhood. The thief steals from the unlocked car in the neighborhood.