3 Simple strategies attorneys can use to improve their law firm’s data security

Data Security

It’s an unpreventable disaster.

One hundred six million people have been affected by the Capital One data breach. A former Amazon employee exploited a vulnerability in Capital One’s cloud system using it to steal sensitive personal and financial data from their customers.

There’s no way anyone could have seen this coming.

There’s just one problem with this belief. It’s completely untrue. A Wall Street Journal report shows the vulnerability that led to the Capital One hack was known (and shared) by security researchers since 2014. It’s no surprise; criminals frequently target financial organizations.

What about law firms?

Which industry is more appealing to cybercriminals?

If you guessed law firms, you're right.

News outlets like the BBC and the WSJ state that law firms are a favorite target for cybercriminals. A report by Recorded Future lists state-sponsored attacks on law firms from China, Russia, and Iran are on the rise. Land a large client and you become a target for cybercriminals. Wait a minute. The majority of law firms are small. Many of them serve individuals or other small-to-medium businesses?

How are these firms at risk?

The ABA TechReport shows most attacks are directed at small and medium sized firms.

- **27 percent** of attacks were directed at firms with *2 – 9 attorneys*
- **35 percent** of attacks were directed at firms with *10 – 49 attorneys*
- **33 percent** of attacks directed at firms with *50 – 99 attorneys*

As far as cyber criminals are concerned, small law firms are the low hanging fruit. They're easy pickings for criminal opportunists looking for an easy payday.

Why?

- **Law firms have a treasure trove of data.** They have client, firm and customer data in the form of agreements, documents, contact details, insider information, personal and financial documents.
- **Law firms have deep pockets.** Cybercriminals assume law firms have a significant amount of cash on hand in the form of hourly billings or cash in a client's trust account.
- **Law firms are exposed and vulnerable.** A LogicForce report listed 4,169 publicly confirmed breaches since 2016. That number is increasing rapidly. What's worse, 40 percent of firms ***weren't even aware*** an attack had occurred.

Law firms act as indirect information brokers. They're expected to safeguard their client's business. Sure that's not your core business. You're focused on taking care of your client's legal matters. But that doesn't matter to these cybercriminals.

You have client data and they want it.

What law firms can do to improve data security

As information brokers, law firms can take precautionary steps to ensure that the information in their possession, law firm and client data, stays in their possession. Aren't most firms doing this already?

Not at all.

A recent report from LogicForce had some surprising implications.

- **53 percent** didn't have a data breach response/recovery plan
- **77 percent** of firms didn't have cyber insurance
- **95 percent** of respondents were noncompliant with their own cyber policies
- **100 percent** were noncompliant with their client's policies

The vast majority of law firms are vulnerable to a data breach. That's obviously bad news for law firms. But it's also *very good news* for law firms.

Here's why.

These vulnerabilities provide law firms with the clarity and direction they need. Let's take a look at some of the steps law firms can take to secure their data.

1. Create a cybersecurity policy

A cybersecurity policy outlines the systems, procedures needed to guard your data against attacks. This policy provides firm-wide direction outlining:

- Who is responsible for what
- Who has access to what (and when)
- How your data should be protected
- Who is responsible for protecting firm data

Your cybersecurity plan should include instructions on **(a.)** the security programs you'll need to implement (e.g., antivirus, firewall, and anti-exploit software). **(b.)** how hardware and software patches or updates will be applied. **(c.)** how your data will be backed up when it will be backed up and where.

2. Move to the cloud

The implication here is this: The majority of small to medium firms aren't prepared for a data breach. This isn't because law firms are somehow inadequate or lazy.

Not at all.

It makes sense that many firms aren't prepared for the inevitable disaster. First, there's cost. Here's what you'll need to spend to build your own IT department.

Title/Role	Small	Medium	Enterprise
Network Operations Manager	$109,260	$123,729	$139,641
Network Administrator	$69,782	$79,194	$89,733
Help Desk Support Rep	$49,248	$55,123	$62,368
Installation and Maintenance Technician	$88,978	$106,212	$126,511
	$317,268	**$364,258**	**$418,253**

These numbers are only focused on employee salaries; they don't include benefits, bonuses or incentives. It also doesn't include:

- Laptops, mobile devices, and other hardware
- Software licenses and setup fees
- Consistent data backups, maintenance and archiving
- Internet and network services
- 24-hour support (including higher on-call salaries)

These expenses make a compelling case for law firms to move their operations to the cloud. Cloud-based practice management software, document management platforms and project management tools enable you to offload your network security to a trustworthy provider.

With cloud software, the responsibility rests on your provider's shoulders.

They're responsible for security, backing up your data regularly and maintaining compliance. It's your provider's job to protect your firm from criminal activity, inappropriate access, freak accidents and acts of God. From negligence and mistakes.

3. Create a disaster response and data recovery plan

According to the LogicForce Cyber Security Scorecard, law firms experience a never-ending avalanche of attacks. Their report shows law firms experience:

- **10,000** *network intrusion attempts* per day
- **1,000** *invalid login attempts* per day
- **59 percent** of ***all emails*** are classified as spam, phishing or ransomware

How can cybercriminals keep up this frantic pace? These attacks are carried out by automated scripts or programs. They're equal opportunity predators. While small firms are low hanging fruit predators will pursue firms of any size, specialty or classification. If you have the resources they want they'll search for a way in.

Good data security makes your law firm a hard target

A breach may be inevitable, but data loss isn't mandatory. At some point, these predators will find the "in" they need. Will they find a firm that's protected all of its data or a firm filled with sensitive (and exposed) client data? It's up to you. With a disaster recovery plan in place, you'll have the resources you need to limit the damage done to your business.

It's not a matter of *if* your organization is attacked but *when* and *how hard*. The time to prepare is now. Make security a top priority, utilize data loss prevention tools, be ready. They're coming for you either way.

FREE TRIAL