# Cyber Security for Law Firms Critical to Meet Ethical, Regulatory and Contractual Responsibilities and Prevent Costly Breaches

Law firms make a particularly attractive target for cybercriminals. They store confidential and highly sensitive data for numerous clients. And, as part of the supply chain, they represent a possible access path into the networks of their more secure clients. Thus, cyber security for law firms proves critical.

Consider the value hackers would place on trade secrets or merger and acquisition details held by a business law firm, for example. Or contemplate the damage caused when bad actors gain access to compromising information on public figures. In fact, a ransomware gang in 2020 demanded a $42 million ransom for information they stole from a celebrity law firm.

Not only do law firms have both an ethical and a regulatory responsibility to protect their clients' data, but data breaches can prove costly in multiple ways. Unfortunately, surveys indicate that law firms often employ less than adequate cyber security measures in an increasingly dangerous digital environment.

## Ethical, Regulatory and Contractual Responsibilities

The American Bar Association Model Rules specify that lawyers use "competent and reasonable measures" to protect client data on technology. They also require that attorneys communicate with clients about the use of technology and obtain informed consent. And they mandate that attorneys supervise both staff and service providers to ensure security compliance.

Competent and reasonable efforts, for example, include implementing basic cyber security best practices such as encryption and endpoint protection. They also include conducting periodic risk assessments to ensure supply chain cyber security. And according to a 2018 formal opinion from the ABA, they include notifying clients when a breach occurs.

In addition to ABA rules, law firms must also comply with regulatory and contractual requirements. For instance, any attorney associated with a health care provider must comply with HIPAA regulations mandating the protection of personal health information from inadvertent disclosure.

Likewise, clients demonstrate an increased focus on data security. Consequently, contracts now frequently include clauses mandating third-party security assessments and implementation of other security measures.

## Law Firm Data Breaches Prove Costly

While ransom demands have risen to staggering heights, the consequences of law firm data breaches extend beyond possible ransoms. For example, in 2016 the law firm Moses Afonso Ryan Ltd. suffered a ransomware attack that locked down crucial files for three months. That meant the firm could not access important financial information or bill clients.

Other costs of a data breach include legal fines incurred, as well as the loss of billable hours. The firm may need to replace hardware or software and pay to upgrade security tools and repair damage. More difficult to quantify, but arguably more costly, is the damage to the firm's reputation and the loss of client and public trust.

## Commit to Cyber Security for Law Firms Best Practices

The ABA technology surveys show that more than one out of every four practices have already experienced a data breach. Common cyber threats faced by law firms include phishing attacks, ransomware, sensitive data leaks, cyber security malpractice allegations and attacks on remote devices.

To counter these threats, law firms must regularly revisit their security strategies. Critical basic cyber security best practices for law firms include the following:

- Start with a **risk assessment** – Regular risk assessments shine a light on security gaps within the organization. This allows the firm to proactively address vulnerabilities before a breach occurs.
- Draft and enforce an **acceptable use policy** – These policies include guidelines for data retention and encryption, as well as appropriate use of email and other platforms. They also specify BYOD policies and may include a blacklist of prohibited internet sites. Automate these policies where possible.

- Build an **incident response plan** – Long before a security incident occurs, prepare a detailed incident response plan. This includes identifying team member roles and detailing regulatory responsibilities. It also spells out procedures for infection containment and eradication and outlines recovery and communication plans.
- Implement **endpoint security** – A mobile workforce broadens the attack surface. Strengthen endpoint security to detect and manage devices and monitor for unusual behavior.
- Reinforce **authentication and access controls** – Evaluate and update the firm's policies and tools governing user access to data, devices, and the network. For example, implement multi-

factor authentication where possible and limit user access to only the data and services needed to complete their assigned tasks.

- Implement **data and device encryption** – Invest in encryption on multiple levels. This includes encrypting emails, servers and devices. Ensure that data is encrypted both in transit and at rest.
- Provide regular, engaging **security awareness training** – In the end, humans represent both the weakest link and the most important defense. Make sure all employees understand their role in ensuring data security.

## Cyber Security for Law Firms Resource

The legal cyber security consultants at eMazzanti Technologies understand the challenges law firms face. Beginning with a risk assessment, they will help your firm build a security strategy tailored to your needs and budget.