8 Law Firm Cyber-Security Best Practices

In 2015, an anonymous source leaked 11.5 million documents stolen from the Panamanian law firm Mossack Fonseca. The client information included in the leak affected over 200,000 entities in more than forty countries. Incidents like this highlight the need for a focus on law firm cyber-security.

The law firm closed because of the scandal, which also resulted in the resignation of various high government officials. Just one year later, news reports broke that hackers had stolen information from as many as 48 major law firms, using that information to gain millions of dollars through insider trading. I could go on.

Cyber-Crime Targets

Because they hold vast amounts of sensitive client and financial data, law firms represent desirable targets for cyber-criminals. In fact, a 2018 survey conducted by the American Bar Association reported that nearly 20 percent of law firms have experienced a cyber-attack. And hackers have increasingly begun to turn their attention to small law firms.

Surprisingly, the legal industry has proven slow to adopt sound cyber-security. Furthermore, migration to the cloud, insufficient access management and the prevalence of bring-your-own-device (BYOD) policies have all increased the danger.

To guard against attack and protect sensitive information, firms should adopt these law firm cyber-security best practices:

1. Ensure Encryption

An essential element of law firm cyber-security involves encrypting data both in transit and at rest. This means that all data transfers, including email, should be encrypted. In addition, encrypt data where it resides, whether on-premises or in the cloud.

2. Back Up Data Regularly

Perform regular backups of any data you cannot afford to lose, and store the backups off-site. Cyber-criminals see law firms as lucrative targets for ransomware. In a ransomware attack, the perpetrators encrypt vast amounts of data, often charging millions of dollars for the decryption tool. Organizations without backups that choose not to pay the ransom lose data permanently.

3. Institute Records Retention Policies

Documents add up quickly in a law office. Many firms mistakenly assume that clients expect them to hold information indefinitely. But holding onto enormous amounts of data not only proves costly; it also presents a security risk. Hackers cannot compromise information that no longer exists.

Determine the regulatory requirements that apply to your organization and to the data you hold for clients. In addition, discuss with your clients the expectations they hold for document retention. If there is no business or legal reason to retain data, remove it.

4. Conduct Risk Assessments

Perform regular security audits to determine vulnerabilities in the system. Those audits will likely include penetration testing of the website and network. They will also involve a review of security policies and procedures and a check of physical systems. Be sure that your policies cover risky areas such as cloud usage and bring-your-own-device (BYOD) scenarios.

5. Verify Vendor Security

Even if your own organization maintains vigilant cyber-security, vulnerabilities in third-party vendors can still threaten sensitive client information. For example, in the massive data breach that affected Target in 2013, hackers compromised Target's system through a vendor in the supply chain.

Thoroughly vet all vendors. Determine which of your vendors deal with confidential information or have access to your network. Make sure contracts cover security issues dealing with that access.

6. Use and Update Basic Security Tools

This should go without saying, but time and time again, organizations lose data because they failed to implement basic security tools. At a minimum, make sure you have anti-virus and anti-malware protection on all devices, including mobile devices. Install updates as they become available.

7. Remember the Human Factor

The human element remains a top contributor to law firm cyber-security risk. Phishing schemes continue to trap employees into downloading malware. And the best security policies mean nothing unless staff follow them.

Train staff regularly to recognize and guard against security risks. Make sure they know policies and procedures. And, where possible, automate those procedures to minimize the chance for human error. For instance, Office 365 controls allow administrators to regulate the sharing of documents outside the organization.

8. Engage a Trusted Cyber-security Partner

A data breach often spells disaster for a law firm, from the immediate loss of intellectual property to long-term loss of client trust. Bringing legal IT security experts on board will deliver the peace of mind you and your clients need to focus on core business goals.

eMazzanti Technologies ranks among the leading legal technology vendors, providing comprehensive cyber-security solutions, as well as cost-effective managed services. Our trained and certified legal IT experts can help your firm implement best practices to ensure the security of sensitive information for both you and your clients.