centerbase.com

Centerbase CloudBased Law Firm Management & Growth Platform

Data Security for Law Firms: Everything You Need to Know

developers · Saturday, April 11th, 2020

2019 was the worst year on record for data breaches, according to at least one research firm. But 2020 already looks poised to eclipse it: data security for law firms and privacy threats have only increased with so many people social distancing and logging into work remotely.

For instance, the World Health Organization recently advised that “hackers and cyber scammers are taking advantage of the coronavirus disease (COVID-19) pandemic by sending fraudulent email and WhatsApp messages that attempt to trick [recipients] into clicking on malicious links or opening attachments.” When users fall for the trap, cybercriminals steal their username and password. Now Zoom bombers are hijacking teleconferences to harass participants and share illicit materials.

Yet there are more than external risks facing us during this pandemic: employees don’t always make the best choices—whether consciously or inadvertently—to protect their data. Often, that’s because they don’t know how to secure their information or because the methods for securing data are cumbersome. But those errors can have devastating consequences. For example, thousands of recorded video calls were (briefly) visible to everyone on the open web. And one healthcare organization jeopardized 344,000 healthcare records because it forgot to wipe the hard drives when the lease on its photocopiers expired—resulting in a civil penalty of $1.2 million.

For lawyers, the consequences of failing to secure data are dire on multiple fronts. Not only might they lose their own data, but they may also lose their clients’ sensitive and confidential information, jeopardizing their attorney-client privilege and violating their ethical duties. These concerns have typically made lawyers loath to let their data out of their sight—or off their in-house servers. But law firms themselves have a poor track record of protecting their data. Perhaps the most notorious law firm breach involved an email hack in 2016 of Panamanian firm Mossack Fonseca, which lost 11.5 million sensitive client records and 2.6 terabytes of data, but other reports suggest that as many as one in four law firms have lost data through breaches.

Now, even for the most cloud-averse law firms, CDC guidance and state mandates have forced their hand. To do any work, lawyers must remotely log in to their firm servers through their laptops and mobile devices. Outside their firm’s cybersecurity infrastructure, firewall, and network security hardware, their data may be more vulnerable than ever. That’s why it’s critical for law firms to understand data security risks and partner with organizations committed to following best practices to protect their data.

Lawyers' Obligations to Maintain Data Security and Privacy

Multiple rules of the American Bar Association's Model Rules of Professional Conduct require lawyers to take steps to protect client data. The duty of competence outlined in Model Rule 1.1 requires that lawyers "understand technologies that are being used to deliver legal services to their clients . . . [and] use and maintain those technologies in a manner that will reasonably safeguard property and information that has been entrusted to the lawyer." Further, Model Rules 5.1 and 5.3 impose the "obligation to safeguard and monitor the security of electronically stored client property and information."

The ABA Standing Committee on Ethics and Professional Responsibility has taken these obligations further in its formal opinions. It states that lawyers must not only protect client information but also notify clients if their data has been compromised in a data breach.

For example, Formal Opinion 477R requires lawyers to understand how they store client data and how it can be accessed, so that they can "manag[e] the risk of inadvertent or unauthorized disclosure of client-related information." Lawyers must ensure that they have implemented appropriate safeguards to limit access to client information and supervise third parties that handle client data, confirming that all third parties take measures that satisfy the lawyer's professional obligations. To fulfill their ethical duties, lawyers should review their vendors' cybersecurity credentials and audit their security policies and practices. Formal Opinion 483 requires lawyers to monitor for potential breaches and take steps to stop and/or mitigate any breach and to notify clients and former clients of any data compromise.

It is clear that lawyers must safeguard their clients' data, regardless of whether it is stored on their own systems or elsewhere. But what exactly are they protecting against?

Law Firm Data Security and Data Privacy Risks

Law firms store a veritable treasure trove of data that any cyberpirate would covet:

- intellectual property protected by patents and trademarks;
- business strategies, including details on potential mergers, acquisitions, and other corporate transactions;
- legal strategies, including litigation, investigation, and compliance tactics;
  personally identifiable information, including benefits and HR details for firm and clients' employees;
- payment data for employees and clients; and
- other sensitive information protected by the attorney-client privilege and as attorney work product.

Because law firms store all of this data for multiple clients, they represent the perfect target for a one-stop data breach—a target that's made even more alluring because many firms lack the state-of-the-art security that other industries have implemented.

Then there are the risks associated with internal threats: employees or contractors may have access to firm and client data, but should their interests diverge from those of the firm, they may take advantage of an opportunity to seize valuable data for inside trading or other nefarious purposes. Or they may not have ever been trained to identify and avoid potential threats. Or they may simply be careless with their data. It's hard to detect or forestall risks like these, because these insiders

have been—appropriately—granted permission to access sensitive data.

What's a law firm to do? The firm's core business is practicing law on behalf of clients—not data security. And, although attorneys are mindful of the need to protect information covered by the attorney-client privilege and work-product doctrine, they aren't experts in IT security or cybersecurity. So, while they may do their best to follow security rules and comply with their ethical obligations in good faith, there's always the risk that something will slip through the cracks.

These are some of the reasons that lawyers should consider sending their information to a cloud-based practice management solution. Here is what you need to know to choose the option that offers the best cloud security for law firms.

What Law Firms Should Look for in a Practice Management Solution

Providers of cloud-based services, including law practice management software, typically offer stronger security than most law firms, because their work centers around data and securing that data. This focus means they continually invest in the latest security tools to guard against evolving cyberthreats.

But not all cloud-based service providers are created equal. Law firms should look for the following data privacy and data security attributes when selecting a cloud-based solution for law practice management.

Physical Security Measures

Your cloud provider's data centers should have comprehensive physical security protocols to prevent unauthorized access. Here are some questions to ask:

- Is the facility staffed and monitored 24/7/365?
- How does the facility monitor physical entry and exit points?
- Does the facility have video surveillance systems, both internal and external?
- Are additional measures, such as keycard access or biometric technology, in place to protect high-sensitivity areas?
- What information does the facility track regarding access events?

Centerbase's data centers follow industry-standard best practices, including checkpoints, gates, fences, 24/7/365 on-site personnel, badge/photo ID access, biometric access screening, secure cages, and full-building video capture. Only individuals on a screened and preapproved list have physical access to our facilities; they must present a pass card to enter the parking lot and undergo a biometric screening to enter the building. An authorized third party is required to physically unlock the cages where your information is stored.

Certifications

What industry-recognized security certifications do the organization and its data centers have? Some of the most common certifications are ISO/IEC 27001, SSAE 18, and SOC 2. Organizations that meet these standards have established that they have adequate controls to securely host data. Make sure a third party has independently audited any organization that you're considering for compliance.

Because your law firm is probably storing a range of data in its law practice management solution, you should also ensure that your provider is compliant with the other laws that you're governed by.

For example, if your law firm works with doctors, hospitals, or other healthcare providers, it is subject to the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act. The HIPAA Security rule and HITECH Act require healthcare organizations and their business associates (those who handle services on behalf of healthcare organizations) to implement administrative, technical, and physical safeguards to shield electronically stored protected health information.

The Gramm-Leach-Bliley Act (GLBA) requires financial institutions and those that collect personally identifiable financial information that is not publicly available—such as names, addresses, income, account numbers, payment history, purchase history, balances, and the fact that an individual is a customer or consumer—to protect that information from disclosure. Covered entities are required to develop an information security program with administrative, technical, and physical safeguards, including measures for detecting and preventing attacks and system failures and selecting third-party providers that offer appropriate data protection.

Depending on the data you collect, your law firm may also be subject to the Payment Card Industry Data Security Standard (PCI DSS). The PCI DSS requires entities that collect credit card data to take steps to protect the systems and devices that store that data, including data centers, with physical security measures and other protections.

Centerbase data centers' compliance with SSAE 18, SOC 1, SOC 2, HIPAA, and PCI DSS v3.2 has been audited by an independent third party.

Disaster Recovery and Business Continuity Plans

What will happen to your data in the event of a cyberattack or other emergency? Any cloud computing provider that your law firm uses should have extensive disaster recovery and business continuity plans that will allow you to resume your business operations after a disaster occurs. Don't take their word for it; ask to see a copy.

Check to make sure that your provider has at least one secondary data center with real-time backup and processing power equal to that of its main site. The backup facility should be geographically and environmentally diverse from the primary data center to avoid simultaneous disruptive events. Ask about uptime statistics, and make sure each data center is protected by battery backup as well as fire detection and suppression systems. Your best bet is a Tier III or higher data center with redundant and dual-powered servers, which allow for maintenance and cooling without any service disruptions.

At Centerbase, we constantly replicate our main site's data to our off-site disaster recovery location to allow for a quick transition in the unlikely event of a catastrophe at our main location. We've operated servers in our main facility for over 14 years without the need for a single failover. We employ a four-tier data redundancy policy, with three encrypted sets at our primary sites and a fourth set at our disaster recovery sites. We have a system-wide 99.999% uptime with zero data loss. We maintain a Tier III offsite disaster recovery location, fully capable of taking over in the unlikely event of a catastrophe at our main data center locations. All Centerbase databases are continuously backed up and can be restored to any point in time within a 10-minute window.

User Authentication and Authorization

How do users access the data in their law practice management system? What processes does the platform have in place to limit access on a need-to-know basis? Does the system have content-level permissions and information rights management protocols? You should be able to set permissions at multiple levels: user, group, and organization. You should also be able to set access independently at the file and folder levels. Finally, make sure your provider offers a complete audit history so you can track logins and monitor access.

Centerbase's advanced application-level security settings allow you to set permissions to any data in the system on an individual or group basis, so you can limit access to financial data, billing rates, sensitive documents, and cases. Our system also includes a user-definable change tracking, audit log, and deletion log system. From an easy-to-use dashboard, you can quickly review all user activity, including changes made, and view both the old and new values and any deletions. You can also monitor logins and log users out remotely. Our server also logs and monitors every connection and communication that is made with your system. We store the IP address, the information that is accessed, and the date and time of all interactions, so you know who is using your system at any time.

Infrastructure Security

How does your provider monitor its perimeter security? Has it implemented antivirus scanning technology? Has it configured a firewall to prevent vulnerabilities such as malware and denial of service attacks? Does it have an intrusion detection system that alerts you to network threats in real time and automatically block attacks? Does it protect data at rest and during transfer with encryption?

Centerbase manages our own firewalls and security policies and has over 14 years of incident-free experience. We design our systems to actively refuse connections from high-risk countries known for hacking activity. We continuously monitor our systems for vulnerability and malicious activity to guard against cyberattacks and DOS incidents. We also employ 128-bit SSL encryption for data transfer, storage, and onsite and offsite backup: in other words, we meet the same stringent encryption standards as financial institutions, healthcare providers, and other security-conscious businesses. This ensures that no one will ever have access your firm's information if they gain physical access to our systems.

Data Ownership

Make sure your service-level agreement with your provider spells out who owns your data: all uploaded data should remain yours. What will happen to your data when the relationship ends? Does your provider have a standard policy to remove data from its servers, archives, and backup devices?

Our clients own all data in our system. When a law firm ends a Centerbase subscription, we make all content available to the firm's administrator or authorized user. All content associated with the firm's subscription is irrevocably deleted from the Centerbase platform within 90 days of termination.

Support

What is your provider’s policy on technical support?

Centerbase keeps a close eye on the performance and response time of your system. Offsite monitoring software constantly reviews our infrastructure for failures or issues. We also monitor each client’s website for response time to ensure a high level of performance. Our staff is notified via text and email when issues arise and are on call and available 24/7/365 to make sure your systems are up, running, and available to you.

Conclusion

Law firms considering a cloud-based practice management and billing solution for the first time may feel some trepidation about losing control of their data. However, by ensuring that their service provider has invested in the measures outlined in this article, they may find that their data is even more secure than in the four walls of their firm.

Curious how we set the bar for legal software security? Check it out here!

This entry was posted on Saturday, April 11th, 2020 at 12:00 am and is filed under Compliance & Security
You can follow any responses to this entry through the Comments (RSS) feed. Both comments and pings are currently closed.