LJN
LAW JOURNAL NEWSLETTERS
LJN's LEGAL TECH Newsletter®
An ALM Publication
Volume 32, Number 10 • February 2016

8 Ways to Secure Your Law Firm in The Ubiquitous Cloud

By Joe Kelly

Much like Donald Trump, Facebook or even the Kardashians, the cloud is everywhere. In our personal lives, it often keeps our family calendars, stores our videos, hosts our e-mails and runs our Fantasy Football games.

In a professional capacity, the cloud is also mainstream. A recent survey of 940 IT business professionals found that 93% of their organizations use the cloud. Mainstream companies such as Rackspace and Amazon thrive by selling managed cloud services. Phone systems run off the cloud, and many popular applications such as e-mail and document storage systems rely on it.

However, for attorneys, the use of the cloud in law firms is a different story. Many lawyers shy away from relying on the cloud for professional services due to concerns about privileged information, compliance with regulations or a desire to ensure secure operations.

The hesitation to adopt the cloud is evident in legal surveys. According to the ABA TECHREPORT 2015 (http://bit.ly/1RzLfkg), the use of cloud services stabilized at roughly 31% of respondents, essentially the same as in 2013 and 2014. However, solo practitioners and small firms lead the way when it comes to adopting the cloud and do so at a much more aggressive pace than other law firms.

Another cloud trend for attorneys revolves around third-party file transfer and storage services. Nearly 60% of the survey respondents said they use Dropbox — despite the fact that it can pose a risk to data security.

No matter what the numbers show, though, the cloud will soon be as ubiquitous in legal as it is in other businesses. It's inevitable. As our reliance on the cloud grows, it's more important than ever for lawyers to understand how they connect to the cloud, the evolving risks that apply to them and what questions they need to ask to ensure confidentiality and privacy for their firms and their clients.

The (Really Short) History Of Cloud Computing

The concept of cloud computing hails back to the mid-1900s when corporations created and used multiple terminals to access one mainframe computer. The cloud grew in prevalence in the early 2000s as evolving technology led to better functionality and businesses began to embrace it whole-heartedly.

Today, the scales have tipped with many businesses — and law firms — opting to work and store a majority of information and applications in the cloud as opposed to in-house. This arrangement often leads to cost savings (no need to buy expensive servers and the ability to pay via stabilized subscription costs) and increased convenience (on-demand access to information no matter where you are via mobile devices or off-site connections).

Changing Cloud Standards, Regulations and Ethics

From a legal perspective, attorneys should be mindful of the evolving standards, regulations and ethics around the cloud. That includes changing security standards, as well as remaining in compliance with regulations such as the Sarbanes-Oxley Act, the Health Insurance Portability and Accountability Act (HIPAA; http://1.usa.gov/1jSFZpy) and others. Firms that accept payment via credit card also need to be aware of the Payment Card Industry Data Security Standard (PCI DSS; http://bit.ly/1xz9Rgl), which is designed to ensure that organizations process, store or transmit credit card information in a secure environment.

Attorneys also need to consider their professional and ethical obligations when they move to the cloud. This well-founded concern may have kept many attorneys away from the cloud in the past.

In April, the Professional Ethics Committee for the State Bar of Texas took up the question as it relates to e-mail, an area that many law firms may not think about when considering using the cloud. In Opinion No. 648 (http://bit.ly/1OXLPrn), the committee tackled this question: "Under the Texas Disciplinary Rules of Professional Conduct, may a

Joe Kelly, founder and CEO of Legal Workspace, launched his company after seeing the potential for the cloud in law firm operations. He is also the founder of Business Network Consulting, Ltd., which implements and supports IT solutions for mid-market companies.

lawyer communicate confidential information by e-mail?"

The answer in some cases may require encrypted e-mail for lawyers who handle employment, divorce, and criminal defense matters. "Under the Texas Disciplinary Rules of Professional Conduct, and considering the present state of technology and email usage, a lawyer may generally communicate confidential information by e-mail," the opinion noted. "Some circumstances, may, however, cause a lawyer to have a duty to advise a client regarding risks incident to the sending or receiving of e-mails arising from those circumstances and to consider whether it is prudent to use encrypted e-mail or another form of communication."

Eight Questions to Help Secure Your Legal Cloud Technology

Attorneys should take note of these risks, especially if they are working with the cloud. Failing to ask these eight questions, and understand the answers, could lead to a data breach, loss of data or difficult recovery process if a disaster occurs. That involves asking eight specific questions about the data security of current and potential providers.

Question 1: What protections exist to safeguard data from hackers?

Cloud providers should have an intrusion prevention/detection system in place that monitors unusual traffic on the firm's servers. The system helps to identify and shut down hackers, who constantly search IP addresses looking for weaknesses.

At the same time, providers need to be able to quickly restore access in case an authorized user inadvertently triggers alarms. This can happen when a lawyer or staff member enters the wrong password into a smartphone, and the phone automatically tries to keep logging in to the system.

Providers should also support two-factor authentication, which requires two components every time an attorney logs in. This approach eliminates the chances that a hacker or computer program can log in to a system remotely and randomly create passwords.

Question 2: What firewalls are in place?

Law firms should look for providers that offer enterprise-grade firewalls that are regularly patched. An optimal approach involves having multiple firewalls in place. Multiple firewalls ensure that if one firewall fails, a backup is already in place.

Question 3: Does the server allow for data encryption for e-mail?

Even tech-savvy law firms may not think about the security of their e-mail. But as the Texas State Bar ethics opinion makes clear, a prudent course is to encrypt all e-mail, whether it is residing on the server or being sent and received. E-mail encryption requires a high level of sophistication and expertise, so many providers may not offer it.

Question 4: Has the environment been tested for government and industry security standards?

Along with the usual considerations for maintaining privilege and confidentiality, any law firm with clients that store, transmit or access protected health information (PHI) must comply with HIPAA standards. These standards are rigorous, and the penalties for non-compliance can be steep. If the firm accepts credit card payments, it's also critical to comply with PCI.

Question 5: Are internal and external security scans performed regularly to find vulnerabilities?

Technology is evolving all the time. Hackers evolve their hardware and software too, and they are constantly seeking new ways to attack systems. In order to provide continuous security, providers need to routinely perform security scans. Law firms that must be HIPAA-compliant must conduct internal and external security scans on an annual basis.

Question 6: Does the provider offer contingency plans such as backups?

Providers should have a secondary site for data storage, in case all of the other redundancies fail or a natural disaster, theft or fire occurs. This ensures that data can be easily accessed in case of an issue. Law firms should also check that the provider's backup site has all the same security procedures that the main site does.

In the case of a disaster, firms need to know how long it will take to get back up and running. Depending on the provider, it could be hours or it could be days.

Question 7: What certifications do the provider's employees have?

When the provider's employees have access to your data, they should be specially trained and the provider should have certifications of its security procedures. Those certifications should include information security certifications and training, as well as non-disclosure agreements.

Question 8: Which third parties have access to the firm's hosted environment?

When problems arise with an application hosted on the firm's environment, attorneys need to understand the protocol the provider users. If the application vendor is allowed onto the virtual server, that means a third party could access all of the firm's and clients' data. This is not only risky, but it could also violate HIPAA rules.

Conclusion

Today's lawyers and their clients are inextricably linked to the cloud, whether or not they realize it. That means law firms need to know what data and communications reside there already, how it gets there, and what risks a firm faces because of cloud usage. By asking the right questions, law firms can ensure that they receive all the benefits of the cloud while minimizing the risks.

—❖—