WHITE PAPER

Is the Cloud More Secure Than You Think?

August 2017

the answer company™
THOMSON REUTERS®

Clients entrust their attorneys with their most personal and important materials — tax returns, divorce settlements, intellectual property, lawsuit documents, financial investments, copyrights. Should this information fall into the wrong hands, it could be disastrous for a client and ruin a law firm's reputation.

It's understandable why a law firm would resist putting their data into the cloud: that is, uploading their data to a secure cloud provider. Many firms still rely on tried-and-true storage methods like external hard drives and even locked file cabinets. After all, it seems like every week there's a new story about a company being hit by ransomware, or a massive database hack that exposes the accounts of thousands of customers. Is moving all your vital information into the cloud taking a massive risk?

As it turns out, it isn't. Cloud computing offers far more extensive security than any law firm could provide on its own. Cloud databases lie within intricate, multitiered security networks that are constantly being upgraded and tested for potential weaknesses. There are backups within backups, all meant to protect your information in the event of a hack or a natural disaster.

A growing transformation

At the recent Thomson Reuters VANTAGE conference, Rick Weyenberg, an Azure Cloud Solutions Architect at Microsoft, noted that 70% of CIOs surveyed in 2016 said going forward they would embrace a cloud-first strategy, no longer using the cloud as a supplemental database. This is a substantial change in attitude from just two years before, when a majority of CIOs had considered cloud services as being ancillary. Also, 451 Research expects the compound annual growth rate (CAGR) for cloud computing to be $44.3 billion by 2020, up from $16.9 billion in 2015.

As it turns out, while 60% of Microsoft's Azure customers had preadoption concerns about cloud data security, upon moving to the cloud, 94% said they believed their data protection had increased compared to on-premises security. "We're seeing people trust us more and more," Weyenberg said, noting that Azure works with research hospitals to house such information as genetic markers. "That's as sensitive as information gets."

Yet while about 90% of Fortune 500 companies are using the cloud today, many law firms remain holdouts. There are a number of reasons for this. A firm may still be greatly paper-oriented. Vital information may be stored in tape libraries or on legacy mainframe architecture. The firm may have made substantial investments in database protections and believes that moving data into the cloud could compromise its own efforts. And the firm may not be familiar with current cloud protections and defense protocols, considering the cloud to be as flimsy, security-wise, as a public Dropbox account.

Moving to the cloud will mean a change in perspective, and will likely be a necessary move at some point. Indeed, one that's likely to be demanded by clients. Law firms need to determine what data they need to secure, the costs of doing so in the future, and whether they're truly the best equipped to be the ones securing it.

Gatekeeping your data

Not long ago, it was a simpler world. Law firms kept paper files in locked drawers or in secure storage facilities; papers were shredded once they weren't needed. Digital information was stored in password-protected databases. After catastrophic events like the Sept. 11 terrorist attacks, off-site backup database storage facilities grew in importance. Still, many firms kept most of their vital information in-house, whether in cabinets or servers.

A key question a firm should ask today is: Who is the gatekeeper of my data? Is my data being fully protected?

Law firms need to determine what data they need to secure, the costs of doing so in the future, and whether they're truly the best equipped to be the ones securing it.

What are the barriers — physical and digital — that currently exist between your confidential information and those who want to illegally obtain it? How much of a fail-safe plan does your firm have in the event of an emergency or cyber-attack? If you back up your data into servers that are physically located in your office, is that truly enough protection?

Ruby Lee, a senior product manager at Thomson Reuters, recommends that firms rank their data security in five ways, and then compare the internal assessments to what a top cloud provider offers:

1. **Physical security** — What is the level of security of the location where your data is housed?
2. **Digital security** — What is the strength of your protection against hacks?
3. **Intruder detection** — How soon do you know if you've been compromised?
4. **Disaster recovery** — How soon can you get up and running after an emergency?
5. **Security processing** — How can clients securely access their data?

For all of these areas, she believes that many cloud services should receive five-out-of-five stars, while the legal industry would generally range between two to four stars at best. The reasoning is simple: Even a law firm that's wholly committed to database security lacks the financial and physical resources at the level of many cloud service providers.

Blocking intruders

Take intruder detection and response, for example. Azure routinely runs "war games" with its programmers. These maneuvers involve about 2,000 employees, half of which attempt to hack into Azure while the other half try to detect and prevent the attack. Afterwards, the two teams consult and the attackers disclose any weaknesses they found. Then they run the game again, with the defenders now the attackers.

"We're constantly trying to compromise our own system," Weyenberg noted, with the goal of perpetually finding and correcting any perceived vulnerabilities. No matter what a law firm's size and budget, this sort of routine and intensive threat detection process is beyond their capabilities.

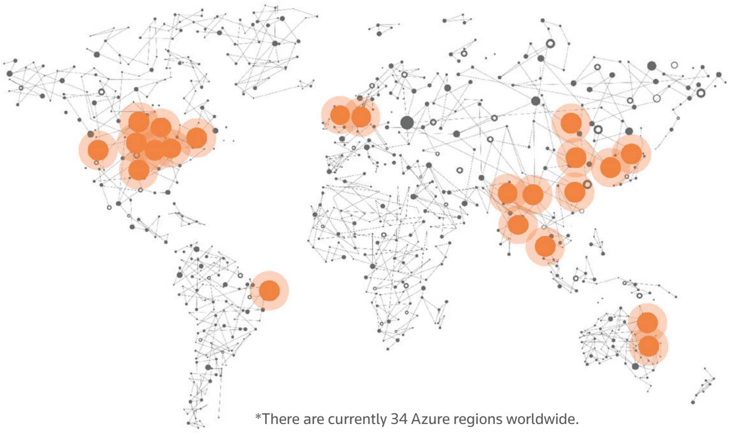
Physical protections

Another likely weak link in a law firm's data security is the location of its servers and databases. Assess what physical barriers exist to protect your data. If your servers are located in your office, who has access to them? Is the security of your office adequate? If servers are located off-site, what protections do their storage facilities offer?

At the same time, many cloud service providers take hardware security as seriously as any government. For example, Azure's cloud servers are housed in facilities that Weyenberg described as being four miles long in some cases, surrounded by military-style fences that extend 25 feet underground. There are various checkpoints within each facility manned by armed guards and surrounded by bulletproof glass. No one gets in without a substantive background check.

Given this imbalance of scale, a law firm's efforts to physically secure its databases and servers will fall short while becoming an unending source of expenses. Even if an off-site storage facility is currently up to date, servers and software protections need continual upgrades. Further, the sheer scale of cloud services can greatly reduce costs for law firms. For example, if your business needs 10 servers running at peak but only one for off-peak hours, in the cloud you can essentially "turn off" nine servers when you're not using them and not pay for them.

If a law firm has clients overseas, there's also the issue of data sovereignty. Some countries like Canada have very restrictive data transfer protocols. Should a firm have to move its data out of a particular country in response to an attack, they could violate that country's regulations. Microsoft has responded by building two cloud facilities in nearly every country in which it does business. Each facility is near a major telecommunications hub and away from fault lines or flood plains. Should one facility be compromised, all client data is automatically secured in the country's other facility: a data transfer that doesn't violate regulations.



*There are currently 34 Azure regions worldwide.
Source: Microsoft®

Encryption: building the digital wall

The ever-increasing complexity of data encryption adds another tier of protection to the cloud. With encryption, as Mark Gendein, architecture manager at Thomson Reuters Elite™, said, "We layer on what we do on top of what cloud providers do."

The overarching idea of encryption is to create a series of impenetrable walls within the cloud. There are no links or connections between various client accounts within a cloud system. Instead, "We create a separate container for each customer. So even if there was a penetration, you still couldn't get from customer A to customer B," Gendein said.

Encryption can be done in a number of ways. A client may use its own encryption service (such as a third-party vendor approved by its cloud provider) or it may ask the cloud provider to encrypt its data. Data is often classified into low-business-impact, medium-business-impact, and high-business-impact. This means that any medium- or high-business-impact data automatically receives additional layers of encryption upon being uploaded, where low-business-impact data receives standard encryption.

Protection from the cloud provider itself

Law firms also should make it clear that their cloud provider itself shouldn't be able to access their data. This is yet another security step, and one that some cloud vendors may overlook. "When you're working with your cloud vendor, you need to know what data, if any, your cloud provider claims ownership to," Weyenberg says. A cloud vendor should be solely interested in providing a platform for a client to build its services on — a big red flag is if they appear to want access to or ownership of any part of your data.

When talking to prospective vendors, firms should ask if privacy controls are built into the provider's design and operations. In the event of an emergency or an upgrade, it may be necessary for a cloud provider to have access to the client's data. If so, this needs to be a very short-term, quickly expiring access for which the client gives express consent.

Make the process work for you

What makes the cloud different from previous generations of digital information storage is in part, the industry knows it needs to prove its security to customers. Convincing clients to move their information into the cloud is still a leap of faith for many, which gives cloud providers extra incentive to keep increasing their security levels and protection protocols.

So, while it may appear to a law firm that moving into the cloud means your data will have more potential for access and exposure, the opposite is true. The name "cloud" itself is something of a misnomer, as the cloud ironically offers more protection than many fortresses on the ground.

A cloud vendor should be solely interested in providing a platform for a client to build its services on — a big red flag is if they appear to want access to or ownership of any part of your data.

For more information, visit: legalexecutiveinstitute.com

The intelligence, technology
and human expertise you need
to find trusted answers.

the answer company™
THOMSON REUTERS®

© 2017 Thomson Reuters S051368/8-17