InsideCounsel

TECHNOLOGY

Cloud Control

Web-based storage offers access, space and speed, but it also brings new risks. BY CHRISTOPHER DANZIG

QUICK READ

- Cloud computing means Internet-based storage
- It's fast, cheap and offers more space
- Security and retention can cause problems

Every day, people across the U.S. flock to the Internet and give their credit card numbers to Amazon.com, eBay or another online retailer. They send myriad personal e-mails using Gmail or any number of other Web-based providers. By doing so, these consumers are all taking advantage of cloud computing. And cloud computing doesn't just affect consumers; it has recently received extensive coverage in the legal world as well. ¶ Cloud computing applies to so many different things that the term can be difficult to define, according to Jeff Davis, a shareholder at Vedder Price. But in its most basic sense, cloud computing is simply any information—including customer data, corporate e-mail or e-discovery production for litigation—stored outside a corporate firewall and accessed via the Internet.

"It's going to cover just about everything," Davis says. "You're going to have every kind of data."

In the business world, he says, everyone seems to be jumping on the cloud computing bandwagon, and it does offer in-house counsel several advantages. But the evolving technology also creates some risks that no one has quite figured out how to manage yet.

Cheap and Easy

Because the cost of data storage continues to drop, cloud computing vendors can offer almost infinitely scalable storage space and fast access speeds for low prices. If companies stored the same amount of data onsite, it would cost significantly more.

Perhaps most importantly, cloud computing allows attorneys across the country—and the world—to access the same data concurrently. This makes work easier in many situations. For example, if several class actions spring up about issues related to the same drug, a single vendor can host the relevant materials in one place, and all the different parties can access it, says Vedder Price Shareholder Bruce Radke.

According to John Bace, research vice president at information technology research firm Gartner Inc., a company can put information in the cloud and its law firms around the country can access

it easily for multiple matters or litigation in multiple cities.

Also, cloud computing creates a way to recover data should a disaster such as a hurricane or earthquake hit a company's main location.

"You want to segregate and distance a backup copy of everything," Davis says. "You want them far away from the primary location, so whatever disaster might hit conceivably would not hit the [backups]."

Keys to the Kingdom

But at the same time, handing everything over to a vendor can be a gamble if counsel doesn't verify the vendor's security and privacy policies.

"Those are the keys to the kingdom, and you've now put them in a place that is unknown, unseen and unmanaged," Davis says.

The first problem is the question of data accessibility and control. Even though the data is not within the company's firewall, technically the company still has possession of the data.

"Even though that information exists somewhere else, as a litigant you have to produce information of which you have possession, custody or control," Radke says.

Not only does a company need to easily produce data for e-discovery, it needs to be able to find and destroy data in line with an established records retention policy. This can be tricky when a company stores data across multiple servers, in multiple locations, and people outside the company manage it.

"What if the destruction date comes up, and some stuff is destroyed and other [stuff] is not?" Davis says. "Later on, when there is a request for document production, but you say everything has been disposed of pursuant to a valid retention program, it [taints] your discovery and your discovery responses."

So it's crucial that the vendor can tell the client exactly what is happening to its data at all times. Ramana Venkata, the chief operating officer at Iron Mountain Digital, a cloud computing vendor, describes how his company handles client data.

"The data has a secure chain of custody," he says. "You need to know who is touching your data. You need to be able to prove nothing bad has been done to it."

Companies using cloud computing also must know where the physical servers holding their data are stored. Different jurisdictions have different data privacy laws that can affect how information can be transferred from place to place (see "Juggling Jurisdictions," below).

Protective Steps

To protect their clients, counsel first need to have strongly worded, auditable contracts with their vendors. Radke recommends working with more established vendors who have had time to work out the kinks in their systems, as opposed to start-ups that might not even survive. (If a vendor goes out of business, that can cause other problems, such as trying to retrieve data from a defunct service provider whose servers are up for sale in a bankruptcy auction.)

Davis also recommends managing cloud vendors as if they were your own staff. "If this was your own department, would you be OK with [the work], or would you be firing somebody?" he says.

The more critical the information that goes into the cloud, the more important due diligence becomes.

Despite all the questions regarding cloud computing, many experts agree there's no avoiding it. So the smartest companies will weigh their options and take advantage of the technology—carefully.

"I don't think this is something you can stay away from," Davis says. "It's inevitable, and frankly it's already here." ■

Juggling Jurisdictions

VENDORS SOMETIMES HOST THEIR SERVERS INTERNATIONALLY, AND IT'S important for in-house counsel to know if a vendor is hosting the company's data in a non-U.S. jurisdiction for several reasons.

To begin with, in regulated industries, hosting abroad might not be legal.

"If you're a U.S. bank, you can't put your data in India, where [regulators] couldn't look at it," says Mayer Brown Partner Brad Peterson, giving one example. European countries often have more stringent privacy regulations than the U.S., so moving data from there to the U.S. might also be illegal. And foreign companies might not want their data stored in the U.S. because the Patriot Act allows the government to look through data for national security reasons.

Finally, litigating in unfamiliar legal systems—especially in developing nations where cloud servers are sometimes hosted—can be complicated, expensive, time-consuming and ultimately futile.

"You'd like to be able to [easily] sue these folks if they don't give your data back," Peterson says.