Business Journal
JACKSONVILLE
25th ANNIVERSARY 1985 | 2010

Jan 14-20, 2011

Finding the legal silver lining to data storage

Advancements in cloud computing technology could help businesses deal with the countless e-mails and other documents employees handle each day — and provide invaluable peace of mind if the company ever faces an audit or litigation.

“You teleport the file instantly, from your device, whether it’s a smart phone or a tablet,” said Michael Cavendish, a partner at the Jacksonville office of Gunster, Yoakley & Stewart PA. “There’s no e-mail, no typing. It’s paperless. You’re teleporting documents like it’s ‘Star Trek.’ ”

Cloud computing, Cavendish said, is “a pretty name for remote data storage that is so seamlessly and devilishly connected it doesn’t feel remote. It feels like magic.”

That “magic” can also help companies organize documents and data. On the cloud, all users work off of one document, instead of e-mailing copies of the document back and forth.

“A key document, like a report — if it’s on the cloud, that’s where the report lives,” Cavendish said. “It isn’t hiding in any weird bin or drawer. If you’ve e-mailed the documents, and you get into a lawsuit or audit, it’s difficult to answer the question, ‘Where is everything we have located?’ It can be blindingly time-consuming to figure it out.”

Cloud cover

Another bonus to storing files remotely, Cavendish said, is that it allows the company to control exactly whom can access the information.

“When you put a file on the cloud, it’s in one place, in one folder,” he said. “[You know which] 15 people have rights to it.”

Whether a business uses cloud computing or a traditional method of data storage, limiting access to documents is a good idea, said **Clinton A. Wright III**, a commercial litigator at **Kelley Kronenberg Attorneys at Law** in Jacksonville.

That way, Wright said, it's easier to keep that information confidential, should it be called into question in a lawsuit.

"You don't want to make the mistake of generally distributing information," Wright said. "Keep it within a subset of people who need to know to do their jobs."

Policies, Wright said, should govern the filing of any document — paper or electronic — that would be of value to a competitor. And although it's never guaranteed, properly labeling and filing that information could prevent it from becoming public.

But the process of organizing a company's electronic documents goes beyond password-protecting certain folders, Cavendish said. It requires a filing system that allows a business owner to say, with absolute certainty, where every document is stored.

JAMES CRICHLOW

Clinton A. Wright III, a commercial litigator at Kelley Kronenberg Attorneys at Law said no matter how you store your electronic data, it's a good idea to limit access to employees who need it to do their work.

It's worthwhile to set aside specific time for employees to organize files and documents, Cavendish said.

"It's a low-priority item," he said. "I don't think it's a matter of irresponsibility; businesses are focused on their No. 1 function: collecting money and dreaming up ways to do it better."

Best practices

For some guidelines on organizing a company's data, Cavendish and Wright offer the following tips:

- E-mail can be one of the biggest information problems in an office, Cavendish said.

“You can achieve a sophisticated level of organization within e-mail programs,” he said. “You can arrange them by sender, by date received, but it’s still not an ideal way to keep things.”

A better way to handle e-mails, Cavendish said, is to organize them into folders, so they’re easier to locate.

“Unless they’ve been through the legal process, most office workers haven’t seen the light,” he said. “Unless someone in the company is an information security evangelist, they don’t even think about these things.”

- Be serious about document protection, Wright said. Do not allow sensitive documents to accumulate. If the documents are on a computer drive, for instance, and a copy is printed just for review, shred the document after review.

- Have a clear company policy about sensitive documents, Wright said, and review it regularly. The policy should define sensitive documents and where they are maintained.

- Compose a nondisclosure/nonuse provision to be included in all employment agreements, in addition to noncompetition provisions, Wright said. The provision should cover the content of confidential or trade secret documents that defines confidential information.

Be sure to include, Wright said, the obligation to keep this information confidential, even beyond the end of employment.

The employment agreement also should require that, if the employee has any company documents in his possession at the end of employment, the documents must be immediately returned to the company.

agurbal@bizjournals.com | 265-2219