Another Red Flag for Fans of the Cloud

Many of you are aware of my staunch opposition to "cloud" software/storage re: law practice/client files, but here is a very ominous article that might shed some light on why:

http://bit.ly/1VutjET

Makes you wonder what those Clio/RocketMatter employees might be doing...

E. Seth Combs, Kentucky

I suppose it makes the point that you should be very careful who you hire. I don't know, however, that Rocket Matter employees can actually access the data. My recollection of how services like Box and Dropbox work is that the data is encrypted on the user's computer, transmitted in its encrypted form, and left encrypted on the remote servers. If the minders of the remote servers do not have keys to decrypt the data, there's no way they could access the information. However, it is a good point to remember that everyone you give permissions to has a key to your data, and you should be very careful who has that.

Dave Armstrong

If you go with the right Cloud service, as Dave says, the data is in a

secure co-location facility, encrypted on the drive and encrypted in transmission. The odds of anyone seeing it that way are fairly slim. On the other hand, the data on your server or computer in your office may not be encrypted. Even if it is, your computer people will always have access as will all of your employees. Further, if you don't have secure passwords and/or your server isn't in a locked room, there is a chance that even the janitorial staff can get to your stuff. I have gone into so many places where the server is in the open, passwords are written on sheets of paper either on someone's desk or right next to the server - or there is a server maintenance book that has at least the admin password, sitting right next to the server. So many small offices are far less secure than data stored in the Cloud.

The issue isn't the cloud, it's how you protect your data. Some of the questions that should be asked when you sign up for a cloud service are - 1) is the data encrypted on the server, 2) is the encryption key stored on the same server or elsewhere, 3) is the transmission encrypted, 4) how is the server protected (I.e. Is it in a locked limited access facility, is it replicated in more than one location, if not, how is the data backed up and what is the prospective down time if a server crashes.

Susan H. Borgos

Did you link to the wrong article? This one has absolutely nothing to do with cloud security - it discusses how your own employees may be stealing your data. That's something that can happen regardless of whether or not you use the cloud - or even whether or not you use computers (employees can

steal paper, after all).

Lisa Solomon, New York

No, I did not link to the wrong article. This has everything to do with cloud security because it highlights the risks that come with a system (cloud or otherwise) in which access is undetectable/undocumented and all of the implications. The point is that there's really no such thing as "the cloud" --- at the end of the day, it's just fluffy language for "another person's computer" and if they have access (physical or otherwise) then, ostensibly, they can peruse, download & transmit, delete, etc. at their leisure without asking you first. Naturally, these companies will promise to have policies/safeguards, but I'm just too jaded when it comes to human nature to rely on any of that.

E. Seth Combs

Exactly right. In the old days, employees walked out with papers in their briefcases. Now they copy data to a flash drive or Dropbox. It's an old problem in a new form. As Dave and Susan said, if you use the right service, the cloud storage provider has literally no way of accessing your data unencrypted.

Rackham Karlsson, Massachusetts

I think the point is that services like Box.com don't leave it to human nature. If a file is encrypted and the employee doesn't hold the encryption key, then they can't peruse, download & transmit, delete, etc., any more than someone who doesn't have a key to a file cabinet can rifle through your files.

Imagine that you're keeping something in storage or a safe deposit box, except the storage company, bank, or post office doesn't even have a matching key to the container. That's what we're talking about.

Rackham Karlsson

"Makes you wonder what those Clio/RocketMatter employees might be doing..." Seth, I like how this attempts to impugn employees at these companies, and the companies themselves, with no basis whatsoever.

Tim Ackermann

Rackham,

I don't disagree with you - it is indeed an old problem in a new form. What I do disagree with is that the solution, categorically, is to simply "pick the right service" unless you can verify the encryption (and its strength or lack thereof) yourself. What I loathe is a) the notion of taking a company's word at face value that "oh yeah, no worries, we encrypt your

data" and b) any service that, by design, requires storage (for any length of time) of files anywhere other than your office PC.

Tim:

I commend your textbook use of the classic straw-man argument by distorting my point as nothing more than a blanket accusation. I enjoyed that. My bumbled phrasing/wording aside, however, I figured you'd be able to see that my overarching point was: remain skeptical about to whom you entrust your data and do not give anyone the benefit of doubt. Not sure about you, but I like to think that pesky 'ol ABA Model Rule 1.6 serves a purpose.
shrug

E. Seth Combs

Seth,

No idea what you are saying here. I made no argument (certainly about your larger point), and I didn't say or suggest that your point was nothing more than a blanket accusation.

Rather I merely pointed out that your comment (hint? sly suggestion?) about people at certain companies doing something wrong appeared to have no basis.

Tim Ackermann

I agree with Lisa, I'm not really sure how the article is related to cloud security.

Seth, you're using an email address. Email is essentially "a cloud." If you've ever sent anyone an email with an attachment, you've essentially used the cloud. Your email provider has that information, including its employees, and the person you sent it to.

As long as you take reasonable care in who you choose as a provider and how you transmit data, the security issues off the cloud are very similar to security issues via cloud-based software.

Sharon Barney

I don't think you should necessarily take the company's word for it.

Box.com at least has been independently evaluated for HIPAA compliance:

http://community.box.com/t5/Account-Information/Box-HIPAA-And-HITECH-Overview-And-FAQs/ta-p/16

There is a limit to how averse we can be to "new" technologies. I regularly encounter clients who share documents with me through Google Drive and other cloud-based platforms. This is how people do business these days, and it is possible to do so with a reasonable level of care.

Rackham Karlsson

Funny (interesting) how they only offer HIPAA compliance to certain levels of customers (enterprise and Elite). ...and place responsibility on Box customers to be compliant. ...or minimize compliance and enforceability of Regulations. There are big-time guidelines under the Final Rule as to what safeguards they need to provide.

On my gosh, where do I begin... I could only scan the whole thing... (perhaps my bad, but really?)

If they are a business associate of an entity subject to HIPAA, then they are subject to HIPAA. I wonder if they sign a client's BAA or will sign only one provided to a client. It matters.

And who did the independent audit? A health law attorney? A consulting company? Someone else?

Sorry... I am not impressed. Yes, they may do more than many cloud based vendors, but is it still enough

Just sayin'...

Amy J. Holzman, Minnesota

"Box applies the same security and privacy controls for all of its customers, whether Personal, Starter, Business, Enterprise or Elite accounts." So, it looks like the requirement to have an Enterprise or Elite account relates mainly to compliance on the customer's end, not on Box's end.

Here is the part that matters most to me and likely most attorneys on this list: "In addition to being able to sign HIPAA Business Associate Agreements (BAAs), Box has the following features in its product as well as

organizational policies" — followed by a long list of security meassures, including encryption in transit and at rest.

I don't have any affiliation with Box.com; it's just what I use right now.

Rackham Karlsson

I think the fundamental point that "there is no cloud" and "you are just using someone else's computer" (or hard drive/server) is 100% correct. Accordingly, I don't care how strong XYZ's security is, I can't disclose confidential information to XYZ. So I won't place any confidential information in any so-called "cloud" server if that means anyone operating that server can read it. It makes no difference to me whether they promise not to.

On the perhaps inadvertent and unintended recommendation of Eric Snowden, I do use SpiderOak. Why? Confidential information gets encrypted before SpiderOak even receives it. SpiderOak may not be the only one to do it that way, but that's the only way to do it, in my view.

John T. Mitchell, Washington, DC

Independent verification of compliance with HIPAA is great, but I just settled a case against a hospital that had independent compliance but they still had an employee go rogue, if you will.

Jonathan G. Stein, California

Just an FYI - the marketing at box.com doesn't match the contracts. See the following excerpt from the Terms of Service and note specifically that they disclaim security. So... buyer beware.

14. NO WARRANTY

BOX PROVIDES THE SERVICE "AS IS", "WITH ALL FAULTS" AND "AS AVAILABLE". TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, BOX MAKES NO (AND SPECIFICALLY DISCLAIMS ALL) REPRESENTATIONS OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, ANY WARRANTY THAT THE SERVICE WILL BE UNINTERRUPTED, ERROR-FREE OR FREE OF HARMFUL COMPONENTS, THAT THE CONTENT WILL BE SECURE OR NOT OTHERWISE LOST OR DAMAGED, OR ANY IMPLIED WARRANTY OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT, AND ANY WARRANTY ARISING OUT OF ANY COURSE OF PERFORMANCE, COURSE OF DEALING OR USAGE OF TRADE. SOME JURISDICTIONS DO NOT ALLOW THE FOREGOING EXCLUSIONS. IN SUCH AN EVENT SUCH EXCLUSION WILL NOT APPLY SOLELY TO THE EXTENT PROHIBITED BY APPLICABLE LAW.

Tatiana Melnik, Florida

We're (mostly) all lawyers here — of course that's what the contract says!

I'm sure they would still be in a world of hurt if it turned out they

weren't actually encrypting data as they claim.

This is fundamentally a question of trust. I trust that Box.com is handling

my data the way they claim, partly because so many other people don't trust

them. They are under very close watch.

Rackham Karlsson