CLOUD SECURITY:

WILL YOUR BUSINESS DATA BE SAFE IN THE CLOUD?

Is the cloud a safe place for your critical business data to be? Cloud security consultant Ara Trembly tells you what you need to know and consider before you decide.

By Todd R Weiss, Tuesday, July 19, 2011

Is the cloud a safe place for your critical business data to be? Cloud security consultant Ara Trembly tells you what you need to know and consider before you decide.

yourself as you review your organizational processes, security concerns and the value and importance of your business data, Trembly says.

"For some businesses, it will be inadvisable to use the cloud," Trembly says. "A business that uses data as its lifeblood" won't want to put that data out there where it would be more vulnerable. "Insurance companies are one of those businesses, as well as financial institutions, medical centers and doctor's offices."

The problem is that if these kinds of businesses don't have their critical data in-house where they can work to maximize its protection and minimize the risks, then they can't be certain that the security is as good as it needs to be. "It's so easy for HIPAA violations to occur. Not that they're all being prosecuted right now, but they could be,"

Will it ever be possible that enterprises with super-critical data security requirements like these could ever use the cloud, whether public or private? Or will these kinds of security challenges make that impossible?

"At the moment I would say no," Trembly says. "The problem with the cloud and with any online application is that online security is really pretty bad and I don't expect that to improve significantly. And the reason it is so bad is that information is sellable, so if someone steals it, they can sell it. I think that some people do say that these problems will be solved eventually, but I don't think so."

That's the real challenge for data security, he says, because the criminals can stay ahead of the white hats who are working to prevent the intrusions and hacks that occur on a regular basis. "They go after Social Security numbers and anything that allow someone to pose as someone else. Anything collected in the realm of industrial espionage is sellable."

And that's what motivates the bad guys, that stream of income, keeping them a step ahead, Trembly says. "They can devote all their time and energy to crack what you do to try to stop them. A lot of these are well-funded criminal enterprises. Just as we make our livings dealing with information and protecting it, they make their livings stealing it."

For these reasons, and their inherent risks, the clients he works with in the insurance and financial service industries "are not comfortable putting things on the cloud."

The cloud security concerns can be present whether you are using a public or a private cloud, Trembly says. In general, I think that things inside your own systems, assuming you have intrusion protection, would be safer. "But if it absolutely has to be as safe as you can make it, you don't use the cloud."

If data-critical businesses absolutely want to use clouds for some of their IT functions, it would be acceptable to use it for non-essential functions such as building maintenance and supply ordering, he says. "Those things have nothing to do with critical data."

Not taking this advice is fine, if you're feeling lucky, Trembly says.

"The cloud has many great aspects to it, with a key benefit being cost savings," he says. But at the same time, saving money isn't worth it if your enterprise is hit with a data breach, which not only causes huge headaches but also costs your company goodwill and its reputation. "Everybody hears about that kind of event. It's all about maintaining trust with this information and if you can't be trusted with it, your customers are going to go elsewhere."

So what should your company do when considering the options? How do you decide whether to consider the cloud or not?

Here are Trembly's top cloud security questions to consider:

1. The key question is, how valuable is your data?

Then you have to ask related questions: What if it was actually breached? Would it shut down the business entirely? Would it cost a lot to recover from the breach? Would it be a public relations nightmare?

"You really have to consider that whole scenario," Trembly says.

2. What you are willing to do to protect your corporate data?

"What kind of investment are you willing to make? Are you willing to bring in and maintain intrusion prevention systems? You have to know the answers to these questions."

3. What changes are you willing to make in your infrastructure and in your policies to make sure that the data is protected?

Trembly says clients are most concerned with and ask how they should set policies about employees and the use of personal devices for work, while still being able to ensure locked-down data protection.

"You have to ask if you are going to standardize on certain portable devices and protect them so you don't have to worry about them, or are you going to let everybody use the devices of their own choice, which is going to be a nightmare for your IT people," he says. "It's something that IT folks are really in a quandary about because the more devices you allow people to use, the more security problems you can have."

You also have to set clear policies that determine and designate which employees can access the secure data and specify if there are limits to their access, Trembly says. "That's a real important one. It's always a good idea to limit access to only those who really need it."

But isn't that already being done everywhere?

"You would think so, but you'd be surprised how often it isn't done," he says.

If you are allowing employees to access any Web site from anywhere inside your firewall, that needs to be changed, according to Trembly. "That leaves you really wide open to malware and those kinds of risks."

"If security is the number one thing on your agenda, then the cloud is probably not a wise move, at least not yet," Trembly says. "That inherent risk is not something I advise clients to take if they are in a business that is data dependent. Generally, what I'm hearing at conferences and from clients is [proceed with] great caution."

Todd R. Weiss covers Enterprise Applications, SaaS, CRM, and Cloud Computing for CIO.com. Follow Todd on Twitter @TechManTalking. Follow everything from CIO.com on Twitter @CIOonline and on Facebook. Email Todd at tweiss@cio.com You can also join Todd in the "CIO Forum" group on LinkedIn.com to talk with CIOs and IT managers about the things that keep them up at night.