the fact that "the cloud" is really just outsourcing. The term "cloud" is simply a catch-all term for subscription-based services running on someone else's network.

May. 12, 2017

With the current break-neck pace of software and technology we can often overlook the fact that “the cloud” is really just outsourcing. The term “cloud” is simply a catch-all term for subscription-based services running on someone else’s network. Evaluating the security of such services requires digging in and asking the provider

some possibly uncomfortable questions. If you aren't currently doing this for each

system.

Our use of a cloud application like this would necessarily mean asking the client to participate. And, even if not actually stated, the fact that we would use it and ask the client to use it, conveys to the client that we "endorse" this software in some way. That means I had to ask the right questions before committing. If we ask our clients to participate in a cloud application, and then down the road that application is breached or found to be low quality, the client will be asking *us* the hard questions.

These are the questions I always ask any potential cloud vendor:

1. What is the security of the facility running the servers?
2. Is client data encrypted? If so, what encryption method is being used?
3. Is the cloud provider's internal system segregated from its internet-facing cloud servers?
4. Does the provider have a security audit they can share with us?
5. What safeguards do they employ on their web service interface and/or API?
6. Do they back up their data regularly and perform test restores for proper disaster recovery?
7. What general data breach and protection policies are in place?
8. Is client data shared with any third parties?

If you can't get satisfactory answers to these questions, deciding to do business with such a provider boils down to a decision about how much risk your firm is willing to take on to gain the potential benefits the service will provide. And, if this is an app for doing client work, you will also be passing on that risk on to your clients. That has to be fully understood at the Partner level.

So, what do I consider "satisfactory" answers to the questions above?

1. **Facility:** Many cloud startups choose AWS, Google or Microsoft for their server

level. For instance, many database servers have an option to encrypt the data in their tables. But, in case of a SQL injection attack, that encryption exists at a lower level and doesn't prevent the data from being accessed.

3. **Service Segregation:** This is a critical piece of knowledge. What you are asking is whether the servers running the cloud application are connected in any way to the cloud provider's own internal company network. Do staff workstations at CloudApp, Inc. have access to the databases and servers used to store client data? If so, something as simple as opening an infected email by a staff person at the cloud app organization could impact the service and client data stored in it. Bottom line is that there should be no integration between those two networks.
4. **Security Audit:** Is the cloud provider in question being audited on a semi-regular basis to a known standard such as SOC1/2/3 or the like? If so, it would definitely go a long way to confirming their security footing.
5. **Service Safeguards**: Any competent cloud provider should be able to provide a document that spells out their basic security protocols. You are looking for such things as password complexity requirements, two-factor authentication, API token granting and revocation processes and account lockout and recovery protocols. In essence, you're asking the cloud provider to explain what hoops a person or application has to jump through in order to gain access to their service. Those hoops should be high.
6. **Data Backup:** This is a no-brainer. You will want assurances that the cloud vendor takes data backups seriously. In 2017 we have already seen two notable cloud services (GitLab and Instapaper) severely impacted by lack of disaster recovery testing. As discussed earlier, being "in the cloud" just means an application or service is hosted on publicly accessible infrastructure. That in no way implies that the data is secure or backed up responsibly. That's up to the provider itself.
7. **Breach Response:** Running and protecting a large cloud service is difficult. Just because a provider has been breached before doesn't mean that they are not trustworthy or competent. What you really want to know is what their response

to a breach looks like. Do they have a policy in place for responsible, timely

the service. As long as the refusal to answer makes sense. For instance, a provider might tell you they definitely hash passwords stored in their database, but for security reasons they don't want to divulge which hashing algorithm they use. I'd be ok with that, as long as the rest of their answers seem competent and pass the "smell test".

Unfortunately, you will run into many startups that refuse to give straightforward answers to these questions. It's not enough that an app works well or solves a problem. If the people running the service don't have enough experience running and protecting such a service reliably at large scale, it's up to us to identify that ahead of time before we commit the data of our firm or our clients into their hands.

———-

Dave Jones is the IT Manager for Pearce, Bevill, Leesburg, Moore, P.C in Birmingham, AL. He has been a network and system administrator in the Birmingham, AL area for 20 years. He has been in the CPA technology field for 18 years. Email: dave@pearcebevill.com; LinkedIn: https://www.linkedin.com/in/daveajones.

Accounting • Auditing • Technology