about whether the cloud is secure persist. Often times these fears are not based on anything specific, just a general comfort level with what we know and what we can see ...

Jul. 28, 2017

Even as the cloud industry grows and adoption becomes more widespread, worries about whether the cloud is secure persist. Often times these fears are not based on anything specific, just a general comfort level with what we know and what we can

see, and a mistrust of things we don't know and can't see. And when it comes to

Regulatory compliance

With all the local, national, international and industry-specific regulations that are in place today, every business has to deal with many different **compliance requirements**. Building your own compliance infrastructure is expensive, and there's a lot at stake if you get it wrong.

Each area of regulation requires specialized knowledge and expertise to maintain compliance. Many areas require periodic audits for third party certification. If you don't pass an audit, you have to go through a remediation process and there is potentially a black mark against your reputation. All of this is more than most companies can afford take on, and it's outside their core competency.

Cloud providers have teams of experts working to maintain compliance in more areas than you probably need or even know about. You get instant access to this compliance infrastructure out of the gate. Their teams of handle all the audits so you don't have to. You can download all the certifications and audit reports you need to demonstrate compliance to your own stakeholders. The costs of the people and technology are amortized across thousands of customers

Authentication

Most people are familiar with authentication, also called identity and access control. We've seen some very big data breaches over the past decade. Poor access control was often the cause. Most companies have difficulty getting this right at a basic level, and can't even come close to what the cloud can provide for advanced functionality and security.

The fundamental problem is the way applications are built. A directory that more or less mirrors the company hierarchy is usually the foundation for giving people

permission to access different systems and documents according to their role. It can

shortcuts, especially with internal applications. There's a temptation to say, "Hey, they're logged in to our domain. That's good enough." That's why we have so many security breaches.

Single-factor authentication requires something you know, typically your name and password. However, **people choose poor passwords** and username/password and login information is relatively easy to steal.

Multi-factor authentication is even harder to implement. It requires something the user knows and something they have, such as a verification code that is texted to your phone, or a link in an email that you have to click. This is a much deeper, more secure process and a very desirable feature.

This is the kind of thing you can get a relatively simple solution for in the cloud. You have directory services, identity governance and security down to the application level. It's all simply a matter of configuration.

Encryption

Encryption is when you systematically scramble data so that nobody can read it unless they have the code key to unscramble it. There are two places that data needs to be encrypted: In transit, when it's traveling back and forth, and at rest, when it's stored. In transit, we have industry standard transport protocols, such as https, which you've seen on your browser. The little lock icon tells you that communication between you and the server is encrypted.

What's also important is encrypting the traffic between internal servers behind your firewall. This is another place where companies take short cuts because encryption requires specialized mathematical expertise, and they believe it's not necessary

because communications and data behind the firewall are secure. That's not

Key management

When you encrypt information, sometimes you have to decrypt it. To do that requires an encryption key, which has to be stored somewhere. The question is where do you store the key? If it's stored locally, there's a risk that internal people can get access and steal it. Most cloud providers offer a service called a key vault, which they manage. It's a very important piece of security infrastructure, again not easy to do well locally.

Threat management

External attack detection is another, separate security discipline, and one where it's hard for an individual company to stay on top of its game. Though the odds of your company experiencing one are small, denial of service (DOS) attacks are a relatively common way to attack a business. A DOS attack could be related to industrial espionage, but there is also a bit of an anarchist hacker community and this is a way they make mischief. The idea is to send so much traffic to your machines that you don't have enough resources to deal with your legitimate traffic. Nothing is breached, but for all intents and purposes your site is unavailable.

If you're managing your own infrastructure, you need resources to both detect and fend off these and other kinds of attacks on your servers. But since this is a once-in-a-blue-moon event for most companies, readiness to respond to these threats is likely to be poor.

However, external attacks are a routine occurrence for a cloud provider. An attack

Vendors like Microsoft and Apple are constantly issuing patches to close these security holes as they are discovered. If your computers are your own, your staff must constantly monitor security advisories and keep patching machines to stay up to date. With cloud services, the hosting provider does all the security bulletin management and patches the machines. They have dedicated staff and processes in place. That's a whole cost center that is no longer necessary for you to deal with.

Server failures

Modern servers are very reliable but individual computers do fail. If for example the hard disk in your server is rated at 5 years MTBF, this means that on average a disk will fail every five years. If you have a dozen servers, you probably don't deal with it very often, but when it happens it's a fire drill. But if you're a cloud provider with hundreds of thousands of servers, you have a dedicated team with a lot of technology at their disposal working on keeping the hardware running all the time. If server starts to exhibit signs of impending failure, they'll move everything to another server and decommission the failing one, most likely without customers ever noticing.

Logging, monitoring, and reporting

You may not be able to see the servers in your data center, but you can see exactly what's going on with your systems at all times, maybe even more than you could if they were on premise.

Cloud providers offer great tools for monitoring what's going on with your infrastructure. You can look at log data, see traffic, who's doing what, and if there were any threats. They have reporting tools for almost anything you'd want to report on. Building that kind of comprehensive monitoring, logging, and reporting

infrastructure in your own environment is expensive and time consuming. With the

None of this is core to your business, and as the saying goes, you can't self security. Your customers simply expect you to have it. They're not going to pay a premium for it, so it will only ever be a cost center.

That's what it really comes down to. There is a cost to getting these things done right. Even large companies with lots of resources are choosing the cloud, because they choose to spend their IT dollars a different way.

Now that you know the specifics, the question really shouldn't be why a firm would put its infrastructure in the cloud. A better question is, why wouldn't they?

———————

Shaun McAravey is Chief Technology Officer and co-founder of Nvoicepay. He has more than 20 years of experience helping organizations make appropriate technology choices by carefully evaluating emerging technologies, and selecting technologies that provide significant technical benefits. Prior to Nvoicepay Shaun was President and CTO of SoftSource Consulting and Chief Technology Officer of STEP Technology. He is also a frequent and entertaining speaker at technical conferences. Shaun has presented at the Microsoft Global Executive Roundtable, Microsoft Global Summit, Microsoft Technical Briefings, SD West and other national developer conferences.

Small Business • Technology

(NASBA) as a sponsor of continuing professional education on the National Registry of CPE