Perspective

A Practical Guide to Cloud Computing Security

What you need to know now about your business and cloud security

Carl Almond

27 August 2009

avanade® Results Realized

From Accenture and Microsoft

Table of Contents

Introduction	3
Internal or External	3
Evaluating Internal IT Security	4
How to Handle Cloud Security Challenges	5
Further Reading	9

Introduction

More so than other types of hosted environments, when it comes to the cloud, companies worry about the "S" word: Security.

There are three important things you need to know about cloud security. First, cloud security is almost exactly like your internal security. The security tools you use every day are the same tools that will be used to protect your data in the cloud. The one difference is that the cloud is a multi-tenant environment with more than one company (multiple tenants) sharing the same cloud service provider.

Second, security issues involving the cloud can all be addressed using your current security tools. Security needs should be carefully considered. But they shouldn't be viewed as a hindrance if you are considering a move to the cloud.

The commodity nature of IT will, over time, require that you move some of your technologies to the cloud to remain financially competitive. So you should begin addressing your security issues and get ready for the move.

Third, if you select a quality cloud services provider, your security in the cloud will be as good as, or better, than your current security in most cases.

Typically, the level of security you get will be designed to meet the needs of the most risky client in the cloud. And, if you use the tools identified in this paper as a starting point, you will have a good idea of how comparable your cloud security versus internal security will be.

IT: Internal or External?

Before addressing the issue of security in the cloud, it may help to address another question first. And that question is not whether to move IT into the cloud, but what should move there. Consider commodities, for example.

Commoditization plays a role in cloud computing. When businesses started taking advantage of IT, the first organizations to computerize their business processes had significant gains over their competitors. As the IT field matured, the initial competitive benefits of computerization fell. Computerization then became a requirement just to stay on a level playing field. In essence, there is an increasing amount of IT that operates as a commodity.

For example, a paper products company needs a certain amount of unique IT to run its business and make it competitive. But it also runs a huge amount of commodity IT. The commodity technology takes time, money, people and energy away from their business of producing quality paper products at a competitive price. As executive management realizes it is operating a lot of commodity IT, which is not core to their competency, the debate shifts from whether cloud computing will take hold in the enterprise to a debate about how much of the organizational IT will be left internal, on premise.

Fictitious Company: Paper Products LLC
Table of commodity IT functions

IT Function	Commodity status	Destination
E-Mail	Commodity	Cloud
File	Partial Commodity	Internal
LAN	Commodity	Internal
WAN	Commodity	Internal
Web Sites	Commodity	Cloud
E-Store	Commodity	Cloud
Portals	Commodity	Cloud
CRM	Commodity	Cloud
Accounting	Partial Commodity	Cloud
Application Dev	Partial Commodity	Internal
Support	Commodity	Internal
IT Architecture	Non Commodity	Internal

To help you determine what parts of your IT can be moved externally, your first tool is the commodity IT analysis form. (See Paper Products table) Use this form to list out all of the functions that your IT organization performs

and if you think this activity is a commodity or not. Then determine where you might place it in the new IT organization. Using our fictional paper products producer, we see that eight of the current IT functions could be considered commodities. Of those, six of them could easily be moved to a cloud provider.

Obviously, our fictional example will not be indicative of your organization. But it can provide you with an organized way of answering your executives when they ask the question about how much of IT needs to remain internal.

Evaluating Internal IT Security

Once you decide what to place in the cloud, it helps to understand the challenges facing internal IT before you face concerns about security regarding adopting cloud computing.

The greatest challenge internal IT faces is the perception by some that it no longer helps businesses differentiate themselves from competitors. When that happens, internal IT is considered a cost center. This devaluing of IT means many organizations fail to adequately fund required budgets to operate a first- class IT infrastructure. In this case, it is only through the herculean efforts of the IT team that a business class IT infrastructure is maintained. Add to this the increasing number of security mandates from external and internal sources, and IT can't fund and operate the organization's IT in the manner required.

The next problem involves specialization and its effect on business function. Businesses exist as specialized entities. An automobile manufacturer, for example, avoids starting a food production business even though it could feed its employees. Why? For an automotive company, producing food products is not their core business. When you look at funding and maintaining a non-core part of the business, it becomes apparent why IT faces a problem.

If we use our automobile manufacturer as an example, it is unlikely that their IT department will be as successful as their auto manufacturing business because it is not core to the business. Conversely, a business that has IT as its only product line, or service, should be more successful at providing first-class IT. So, if an automobile manufacturing company is not going to operate a best-in-class IT business, why would we expect its security to be as good as the best-in-class IT company?

Now let's examine why best-in-class internal IT security is harder to attain than you might think:

First, there are few skilled security professionals.

- The number of highly skilled and experienced security technologists is very small. It's almost impossible to find qualified security personnel. Organizations can have a contract with a security director or Chief Security Officer (CSO) on an as-needed basis to get the breadth of security knowledge required. But most do not.

Second, good security is expensive.

- If your IT operations face trouble getting full funding, how likely will funding for security be available if there is no real ROI--except for the possibility of keeping unexpected problems from happening? Unlike insurance, where you spend money and you get paid for any loss, when you spend on security, any loss you have requires you to spend more money.

Third, your IT and security staff has an interest in the contents of your data.

- Your internal IT and security are your employees. They have an interest in your data. For example, in many organizations, the system administrators have administrative access to the CEO, CFO and legal department's e-mail. Obviously, you trust your current IT people. But how about that new junior

administrator you have to hire next year when one of your current trusted administrators decides to move on to a new position?

Fourth, any resource (employees, contractors, janitorial service workers) in your organization that has access to your datacenter has access to all of your data.

- If someone has physical access to your servers, it takes about 60 seconds to take full control of the servers and start shipping your data out the door. It is unlikely that a non-IT business has the time or resources to keep a fully staffed IT organization around the clock. It lacks the physical monitoring and safeguards required to meet the security provided in a first-class data center.

Fifth, most internal IT organizations grew with the business.

- As the company grew, so did the IT organization and technology capacity. This as-needed growth was good for the business. But it's bad for IT security. Instead of modern architectures, built around best practices, your architecture may be a mesh of what was needed over time. Many organizations still have not implemented an "isolation of systems" policy. This means that different systems share common infrastructure, such as networking, database, storage, etc. This lack of isolation makes a malfeasant's job much easier. When they take control of one machine, they get unfettered access to all machines.

The intentions of internal IT are well placed. But external factors make their job of securing the organizations data an almost insurmountable task, especially when IT is not the organization's core business.

On the other hand, a company that does IT as its business has a much better chance of securing your data. The quality of its product, and its market success, stands on the effectiveness of its security.

How to Handle Cloud Security Challenges

The challenges of cloud computing are very similar to those of any other organization.

Like internal IT, cloud providers have internal and external threats that can be mitigated or accepted. Because of the commodity nature of IT, consumers expect the multi-tenancy aspect of cloud computing to bring their costs down. Cloud providers reduce costs by spreading the

Mini Cloud Risk/Mitigation Table	
Risk	Mitigation
Multi-tenancy	Infrastructure/data segregation
Ever developing risk	Continuing risk assessment program, CSO/CISO, Assessment
Relaxation of security	Periodic assessment/audit
Service provider tiers	Contract pass-through, coordinated security assessment
Contractor access	Background checks, Contracts, Segregation, Surveillance
Disasters	SLA, Multi facility provisioning
External Physical	Secure facility, Escort, Surveillance
External Logical	IPS, Firewalls, WAF, Secure Coding, Secure Architecture, Host hardening
Incidents	Facility & Per Customer Incident Response Plan
Application bugs	Layered security, Patching, Secure coding practices, Assessments, Segregation
Data leakage	Encryption (at rest & in flight), Segregation, Assessment, Host hardening

IT operations cost across multiple organizations.

Multi-tenancy means you may be exposed to a greater level of external risk due to the business practices of the other tenants. When IT is constrained to your organization, your risk is, to some extent, yours alone to bear. But none of the security challenges in cloud computing are insurmountable.

Multi-tenancy

- As long as the cloud provider builds its security to meet the higher-risk client, then all of the lower risk clients get better security than they would have normally. If you are a bandage manufacturer there is a low risk of being a direct target of malfeasants. Whereas, if you are a music label that is currently suing file sharers, you should expect to experience a high risk of being targeted by malfeasants. But, when both the bandage manufacturer and the music label use the same cloud (mulit-tenancy), it is possible that attacks directed at the music label could affect the bandage manufacturer's infrastructure as well. So the cloud provider must design their security to meet the needs of the music label—and the bandage manufacture gets the benefits.

Security Assessment

- Over time, organizations tend to relax their security posture. To combat a relaxation of security, the cloud provider should perform regular security assessments. The assessments should be done by someone who is experienced and able to identify issues and fix them. The report should be provided to each client immediately after it is performed so they know the current state of the overall cloud's security.

Shared Risk

- In many instances, your cloud service provider will not be the cloud operator. But it may be providing a value-added service on top of another cloud provider's service. For example, if a Software as a Service (SaaS) provider needs infrastructure, it may make more sense to acquire that infrastructure from an Infrastructure-as-a-Service (IaaS) provider rather than building it. These cloud service provider tiers that get built by layering SaaS on top of IaaS, for example, can affect your security. In this type of multi-tier service provider arrangement, each party shares the risk of security issues because the risk potentially impacts all parties at all layers. This issue must be addressed by taking into consideration the architecture used by your cloud provider and working that information into your total risk mitigation plan.

Staff Security Screening

- Most organizations employ contractors as part of their workforce. Cloud providers are no exception. As with regular employees, the contractors should go through a full background investigation comparable to your own employees. Your cloud provider must be able to provide you with its policy on background checks and document that all of its employees have had a background check performed, according to the policy. Further, you should contractually bind the cloud provider to require the same level of due diligence with its contractors.

Distributed Data Centers

- Disasters are a fact of life. They include hurricanes, tornadoes, landslides, earthquakes and even fiber cuts. In theory, a cloud computing environment should be less prone to disasters because providers can provide an environment that is

geographically distributed. But many organizations sign up for cloud computing services that are not geographically distributed. So they should require their provider to have a working and regularly tested disaster recovery plan, which includes SLAs. For those organizations that do contract for geographically diverse cloud services, they should test their cloud provider's ability to respond to a disaster on a regular basis.

Physical Security

- Physical external threats should be analyzed carefully when choosing a cloud security provider. Do all of the cloud provider's facilities have the same levels of security? Are you being sold on the most secure facility with no guarantee that your data will actually reside there? Do the facilities have, at a minimum, a man trap, card or biometric access, surveillance, an onsite guard, a requirement that all guests be escorted and all non-guarded egress points be equipped with automatic alarms?

Policies

- Any organization that says it has never had a security incident is being deceptive or is unaware of the incidents it has had. It is unrealistic to assume a cloud provider will never have an incident. Cloud providers should have incident response policies. And they should have procedures for every client that feed into their overall incident response plan.

Coding

- All cloud providers still use in-house software, which may contain application bugs. So every customer should make sure that the cloud provider follows secure coding practices. Also, all code should be written using a standard methodology that is documented and can be demonstrated to the customer.

Data Leakage

- Data leakage has become one of the greatest organizational risks from a security standpoint. Virtually every government worldwide has regulations that mandate protections for certain data types. The cloud provider should have the ability to map its policy to the security mandate you must comply with and discuss the issues. At a minimum, the data that falls under legislative mandates, or contractual obligation, should be encrypted while in flight and at rest. Further, a yearly risk assessment just on the data in question should be done to make sure the mitigations meet the need. The cloud provider also needs to have a policy that feeds into the security incident policy to deal with any data leakages that might happen.

Conclusion

While security emerges as a major concern among those who respond to cloud computing surveys, the key to understanding security in cloud computing is to realize that the technology is not new, or untested. It represents the logical progression to outsourcing of commodity services to many of the same trusted IT providers we have already been using for years.

Examples of previous "cloud computing" capabilities include hosted mainframes (more than 40 years), hosted file and mail servers (AT&T, IBM in the early 90's), and software services like SalesForce.com.

Cloud computing, which we define as enabling and delivering computing services (computing power, data storage, network bandwidth and application software) over a network on an as needed basis, has been evolving and continues to evolve. So moving IT elements into the cloud becomes a natural next step.

- Cloud computing is the logical move for services to take as more established parts of IT are commoditized. Not moving to cloud computing will mean you are paying more than your competitors for the same commodity.
- Unless your organization is in the business of doing security, it is likely to be less secure than your cloud provider. Work with the provider to determine its attention to security. Compare it to your current levels of actual security to make sure the provider is achieving parity or better levels of security.
- Remember that the security of the cloud should be equal to the most risky client that the provider has.
- Risk assessment is the key to cloud security. Require your cloud computing partner to provide you with its risk assessment and how it intends to mitigate any issues found.
- If the cloud provider does not have a seasoned client-facing CSO, CISO, or equivalent security person, be very careful. It is a sign that it doesn't take security seriously enough.
- Schedule mandatory monthly discussions with the cloud provider's top security person. This discussion should flow both ways with no hidden items.
- The cloud provider should have the ability to map its policy and procedures to any security mandate or security driven contractual obligation you face.
- Pay attention to your cloud provider's adherence to secure coding practices. If it does not have a good story around the discipline it uses to write code, run away.

Cloud security is part of the inevitable progression of IT. It must be embraced by organizations to stay competitive. Companies who approach cloud computing in a mature manner need not be afraid about entering the cloud because of security concerns. Dealing with security in the cloud is no more difficult than addressing it internally. And there are steps you can take that can make cloud security just as effective—or even more so—as your internal IT.

Further Reading

NIST - Effectively and Securely Using the Cloud Computing Paradigm - http://www.govinfosecurity.com/external/reg1388-Cloud.Computing.Primer.pdf

Cloud Security Alliance – CSA Guidance v1.0 - http://www.cloudsecurityalliance.org/guidance/csaguide.pdf

About the Author
Carl Almond is a Senior Director of Security at Avanade. He is a Cloud Security Evangelist.

Americas
Seattle
Phone +1 206 239 5600
America@avanade.com

Europe
London
Phone +44 0 20 7025 1000
Europe@avanade.com

Asia-Pacific
Sydney
Phone +612 9005 5900
AsiaPac@avanade.com