Gartner

Research

Publication Date: 3 June 2008 ID Number: G00157782

Assessing the Security Risks of Cloud Computing

Jay Heiser, Mark Nicolett

Organizations considering cloud-based services must understand the associated risks, defining acceptable use cases and necessary compensating controls before allowing them to be used for regulated or sensitive information. Cloud-computing environments have IT risks in common with any externally provided service. There are also some unique attributes that require risk assessment in areas such as data integrity, recovery and privacy, and an evaluation of legal issues in areas such as e-discovery, regulatory compliance and auditing.

Key Findings

- The most practical way to evaluate the risks associated with using a service in the cloud is to get a third party to do it.
- Cloud-computing IT risks in areas such as data segregation, data privacy, privileged user access, service provider viability, availability and recovery should be assessed like any other externally provided service.
- Location independence and the possibility of service provider "subcontracting" result in IT risks, legal issues and compliance issues that are unique to cloud computing.
- If your business managers are making unauthorized use of external computing services, then they are circumventing corporate security policies and creating unrecognized and unmanaged information-related risks.

Recommendations

- Organizations that have IT risk assessment capabilities and controls for externally sourced services should apply them to the appropriate aspects of cloud computing.
- Legal, regulatory and audit issues associated with location independence and service subcontracting should be assessed before cloud-based services are used.
- Demand transparency. Don't contract for IT services with a vendor that refuses to provide detailed information on its security and continuity management programs.
- Develop a strategy for the controlled and secure use of alternative delivery mechanisms, so that business managers know when they are appropriate to use and have a recognized approval process to follow.

The information contained herein has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner's research may discuss legal issues related to the information technology business, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The opinions expressed herein are subject to change without notice.

ANALYSIS

Gartner defines cloud computing as "a style of computing where massively scalable IT-enabled capabilities are delivered 'as a service' to external customers using Internet technologies." From a security and risk perspective, it is the least transparent externally sourced service delivery method, storing and processing your data externally in multiple unspecified locations, often sourced from other, unnamed providers, and containing data from multiple customers.

This model provides cost savings through economies of scale, but it not only introduces the same risks as any externally provided service, it also includes some unique risk challenges. The word "cloud" suggests something big and accessible, but externally opaque. You can't see into the cloud — you just assume that it works. Obviously, a service provider has far more flexibility by avoiding specifics about its location, staff, technology, processes or subcontractors. Increasingly, service is being offered by a chain of providers, each invisibly offering processing or storage services on behalf of a service provider that might not be directly controlling any of the technology, and each able to invisibly access unencrypted data in its facility. All this makes it easier for them to keep their costs down and scale to meet changing customer demands, but it also makes it harder to assess the risk to your organization from using such a service.

Organizations potentially can gain a competitive or cost advantage through selective adoption of cloud computing, but not without first taking a comprehensive look at the associated risks, ensuring that they are consistent with business goals, along with the expectations of regulators, auditors, shareholders and partners. It is especially challenging to understand the risks associated with cloud computing, and CIOs, chief information security officers, compliance and privacy officers, and line-of-business managers should be involved in the risk assessment of new cloud-based services.

If a company is considering the use of an external service of any sort, then it needs to:

- Assess the security, privacy and regulatory compliance risks
- Identify use cases that are inappropriate for this service delivery method, based on risk level and current controls
- Identify use cases that pose an acceptable level of risk for the service delivery method
- Choose and implement compensating controls before going fully operational

What to Evaluate

Privileged User Access

When sensitive data is processed outside the enterprise, or by non-employees, it means that organizational managers are less immediately aware of the nature and level of risk, and that they have no direct ability to control these risks. Any externally sourced IT service bypasses the physical, logical and personnel controls that IT normally provides for in-house applications. Although it is certainly the case that trusted company employees can make mistakes and commit fraud, and it is not the case that outsiders are automatically less ethical than employees, experienced security specialists are highly aware of the inverse relationship between loyalty and risk. It is only prudent to put a higher level of trust in your fellow employees than in people who do not have a long-term commitment to your organization. Ask providers to supply specific information on the hiring and oversight of privileged administrators, and the controls over their access.

Compliance

Cloud service providers may be new, but we know that most regulations hold the user of the service ultimately responsible for the security and integrity of their corporate and customer data, even when it is held by the service provider. Traditional service providers submit to external audits and security certifications, providing their customers with information on the specific controls that were evaluated. A cloud-computing provider that is unwilling or unable to do this is signaling that customers can only use them for the most trivial functions.

Data Location

A unique ramification of the cloud-computing model is that you probably cannot know where your data is hosted. Indeed, in an increasingly globalized infrastructure, you might not even know in which country your data is stored, which should be of concern to anyone needing to meet national privacy regulations. Will providers commit to storing and processing data in specific jurisdictions? If you are operating within a jurisdiction that has specific privacy requirements, is the provider willing to give a contractual commitment to obey the law on your behalf?

Data Segregation

Virtually all cloud offerings use Secure Sockets Layer to protect data in transit, but most cloud offerings store data in a shared environment. Find out what is done to segregate data at rest. If your data can be read at your provider's site, then you have to assume that it will be read. Increasingly, software-as-a-service (SaaS) vendors are touting the use of encryption for the stored data. Encryption is better than anything else yet devised for preventing unauthorized access to data, but it isn't magic. Don't be distracted by claims of superior key length and choice of encryption algorithm. The most likely failure mode is through an implementation mistake that results in unexpected and exploitable weaknesses. Ask for evidence that the encryption implementation was designed and tested by experienced specialists. Find out who performed the protocol analysis and code reviews. Encryption accidents can make data totally unusable, and even normal encryption can complicate availability. If your data will be stored and backed up in encrypted form, then find out who has access to the decryption keys and whether it is possible for authorized individuals at your company to gain access to their employees' data in an emergency.

Availability

Reliability is one of the core advantages inherent in the cloud-computing model. By its very nature, it is highly scalable, capable of meeting wide variations in processing requirements and insulating users from site problems. However, many cloud-based offerings do not provide service-level commitments that are typically needed for critical business processes. Organizations should define service-level requirements for any nontrivial IT workload and demand service-level agreements from the provider (internal IT, traditional outsourcer, cloud-computing provider) and ensure that the contract contains penalty clauses when service-level agreements are not met.

Recovery

Beyond continuity of operations, organizations need to know how cloud offerings will recover from total disaster. Any offering that does not replicate the data and application infrastructure across multiple sites is vulnerable to a total failure. Even if an offerer refuses to tell you exactly where it will store your data, it should be able to tell you what would happen to your data and service if one of its sites succumbs to a disaster. Does it have the ability to do a complete restoration, and how long will it take?

Investigative Support

Internal investigations of inappropriate or illegal activity, and electronic discovery, are difficult and expensive propositions, even when conducted in your infrastructure. If you are considering purchasing a service that would process anything considered a business record, or if you otherwise anticipate a need to conduct investigations, then you cannot assume that a service provider will be willing, or even able, to support them. Cloud services are especially difficult to investigate, because logging and data for multiple customers may be colocated and may also be spread across an ever-changing set of hosts and data centers. If you cannot get a contractual commitment to support specific forms of investigation, along with evidence that the vendor has already successfully supported such activities, then your only safe assumption is that investigation and discovery requests will be impossible.

Viability

The long-term viability of any external service provider is also something that needs to be evaluated. What would happen to your service if the provider goes broke or is acquired? What assurance can it offer that this won't happen, or if it does, that you will be able to use your data? Ask potential providers how you would get your data back and if it would be in a format that you could import into a replacement application?

Support in Reducing Risk

Evaluate the information and support provided to enable customer staff to understand how to safely and reliably use their product. Are instructions provided to administrators and managers for setting and monitoring policies? Are users provided with instructions on how to avoid phishing or malware attacks?

How to Assess

Ask these questions to evaluate the security and continuity risks associated with a cloud offering:

- How qualified are the policymakers, architects, coders and operators to understand and reduce the risks of their offering?
- What risk control processes and technical mechanisms are used?
- What level of testing has been done to verify that the service and control processes are functioning as designed and to identify unanticipated vulnerabilities?

In practice, there are only three ways to answer these questions and provide a risk assessment of a service:

1. Accept whatever assurances the service provider offers.
2. Evaluate the service provider in person.
3. Use a neutral third party to perform a security assessment.

The first method is obviously not the most rigorous or defensible, but it is the one most often used, and often for good reason. Many organizations have no ability in-house to adequately assess the security of a sophisticated offering, so they seek out suppliers that have more security and continuity expertise than they do. Unfortunately, many of today's cloud-computing products only come with the vaguest information about risk controls. Do not accept unsubstantiated claims, such as "we follow best practices," or vague assurances, such as "our employees are not reading your mail." Ask for specific evidence that answers questions on qualifications, controls and testing. Ultimately, you cannot expect any commercial organization to be totally objective about its weaknesses. To be fully transparent, a provider needs to be willing to undergo external reviews.

Those organizations that are most concerned about the risks associated with their suppliers, if they have the resources and expertise, may send a team of their own people to conduct an on-site assessment. This is common when a global bank sets up an offshore service center, but it is rare for a cloud-computing scenario. Organizations with highly regulated data doing multimillion dollar service buys will continue to perform some level of risk assessment on their service providers' sites, but this is an expensive and inefficient process for both partners, and it is virtually never an effective assessment method for cloud computing.

The most practical way to evaluate the risks associated with a cloud-based service is to get a third party to do it. A specialist security firm can often provide a higher level of rigor than any but the most sophisticated of clients. One assessment or certification firm can do a thorough risk analysis, and this single assessment can satisfy the needs of multiple customers, which dramatically reduces the cost. Furthermore, the third-party assessor is less biased than the first-party customer and especially less biased than the second-party cloud provider. Neutrality is more reliable, and it is more defensible. Ultimately, certification will become the norm for cloud offerings. Although relatively few of the emerging cloud-based services have typical certifications, many of the more established SaaS offerings have been certified. It remains to be seen whether International Organization for Standardization 27001, SysTrust or perhaps some new, purpose-designed certification will prove most useful. Statement on Auditing Standards No. 70 is generally not appropriate for the generic types of services being offered in the cloud, although it is being used as a form of third-party risk assessment for SaaS offerings, especially those that are more relevant to Sarbanes-Oxley regulated data.

Transparency

Ultimately, your ability to assess the risk of using a particular service provider comes down to its degree of transparency. Cloud-computing offerings that include verifiable and specific information about security and uptime are easier to assess, providing a competitive advantage over those that do not. The best practices for cloud computing will undoubtedly include a high level of transparency, but it is not yet clear exactly what forms this will take. One interesting early example is trust.salesforce.com, a site that salesforce.com is providing to show its current and historical uptime statistics. The site also provides information on security alerts and instructions to end users in how to avoid phishing attacks. It is obviously not a complete guide to the risks associated with using salesforce.com's product, but it not only acknowledges that users of the service can be compromised, it also provides concrete information about uptime performance. The less information that is hidden, the easier it is to trust a provider.

Conclusion

Business units and IT organizations should evaluate the business benefits and risks of cloud-based products. As the name "cloud computing" suggests, implementation and operational details, such as location, are irrelevant, which is a wonderful efficiency. Unfortunately, this is not a delivery model that is easily risk-assessed, and there are situations in which cloud computing cannot be considered acceptable without a higher level of assurance than is currently provided. Organizations that demand the ultimate in transparency will find that their IT organization is innately more transparent than any external provider can ever be. Organizations need to evaluate cloud-computing risks, identifying appropriate controls and use cases.

RECOMMENDED READING

"Toolkit Presentation: Integrating Privacy and Security Requirements Into Sourcing Relationships"

"How to Manage Risk in Alternative Delivery Models"

"Critical Security Questions to Ask a SaaS Provider"

"Assessing Outsourcing and Third-Party Security Risks"

"Use Privacy and Security Practices and Contract Terms as Essential Evaluation Criteria of Your Global Service Provider"

"Package Implementation Using ESPs: Critical Success Factors and Risk Framework"

"Identity Services (in) the Cloud"

This research is part of a set of related research pieces. See "Cloud Computing Confusion Leads to Opportunity" for an overview.

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters
Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters
Gartner do Brazil
Av. das Nações Unidas, 12551
9° andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509