IBM Global Technology Services
Thought Leadership White Paper

November 2010

Strategies for assessing cloud security

IBM

Executive summary

Cloud computing provides flexible, cost-effective delivery of business or consumer IT services over the Internet. Cloud resources can be rapidly deployed and easily scaled, with all processes, applications, and services provisioned on demand, regardless of the user location or device. As a result, cloud computing helps organizations improve service delivery, streamline IT management and better align IT services with dynamic business requirements. Cloud computing can also simultaneously support core business functions and provide capacity for new and innovative services.

Both public and private cloud models, or a hybrid approach using both models, are now in use. Available to anyone with Internet access, public clouds are acquired as a service and paid for on a per-usage basis or by subscription. Private clouds are owned and used by a single organization. They offer many of the same benefits as public clouds, but give the owner greater flexibility and control.

Although the benefits of cloud computing are clear, so is the need to develop proper security for cloud implementations—whether public or private. Embracing cloud computing without adequate security controls can place the entire IT infrastructure at risk. Cloud computing introduces another level of risk because essential services are often outsourced to a third party, making it harder to maintain data integrity and privacy, support data and service availability, and demonstrate compliance. Even if IT workloads are transitioned to the cloud, users are still responsible for compliance and data security. As a result, subscribers must establish trust relationships with their cloud providers and understand the risk posed by public and/or private cloud computing environments.

Security challenges in the cloud—the need for a trusted third party evaluation

One of the most significant differences between cloud security and traditional IT security stems from the sharing of infrastructure on a massive scale. Users spanning different corporations and trust levels often interact with the same set of computing resources. And public cloud services are increasingly being offered by a chain of providers—all storing and processing data externally in multiple unspecified locations.

Inside the cloud, it is difficult to physically locate where data is stored. Security processes that were once visible are now hidden behind layers of abstraction. This lack of visibility can cause concerns about data exposure and compromise, service reliability, ability to demonstrate compliance and meet SLAs, and overall security management.

Visibility can be especially critical for compliance. The Sarbanes-Oxley Act, the Health Insurance Portability and Accountability Act (HIPAA), European privacy laws, and many

other regulations require comprehensive auditing capabilities. Many public clouds may indeed be a black box to the subscriber, thus clients may not be able to demonstrate compliance. (A private or hybrid cloud, on the other hand, can be configured to meet those requirements.)

In addition, providers are sometimes required to support third-party audits, or support e-Discovery initiatives and forensic investigations. This adds even more importance to maintaining proper visibility into the cloud. Legal discovery of a co-tenant's data may affect the confidentiality of other tenants' data if the data is not properly segmented. This may mean that some sensitive data may not be appropriate for certain cloud environments.

Organizations considering cloud-based services must understand the associated risks and ensure appropriate visibility. IBM guidelines for securing cloud implementations focus on the following areas:

- Building a security program
- Confidential data protection
- Implementing strong access and identity
- Application provisioning and de-provisioning
- Governance audit management
- Vulnerability management
- Testing and validation

Because cloud computing is available in several service models (and hybrids of these models), each presents different levels of responsibility for security management. Trusted third parties can help companies apply cloud security best practices to their specific business needs.

Developing a strategic cloud security roadmap with IBM

There is no one-size-fits-all model for security in the cloud. Organizations have different security requirements that are determined by the unique characteristics of the business workload they intend to migrate to the cloud or the services they are providing from their cloud. It is important when evaluating risk in a cloud computing model, that a cloud security strategy be developed.

By partnering with IBM, clients can benefit from proven assessment methodologies and best practices that help ensure consistent, reliable results. They can also leverage comprehensive frameworks that address enterprise cloud strategy, implementation and management in a holistic approach that maximizes the business value of cloud investments while minimizing business risk.

Defining business and IT strategy

The first step to understanding security risks posed by a cloud computing model is to analyze business and IT strategies. What is the value of the information that will be stored, accessed and transmitted via the cloud? Is it business critical and/or confidential? Is it subject to regulatory compliance? Clients must also consider availability requirements. After determining the business and IT strategy and evaluating the data, clients can make a more informed, risk-based decision about which cloud computing model to pursue.

Identifying the risks

Each type of cloud—public, private and hybrid—carries a different level of IT security risk. Security experts from IBM can help clients identify the vulnerabilities, threats and other values at risk based on public, private or hybrid cloud architecture. From there, IBM will work with clients to design initial mechanisms and controls to mitigate risk, and outline the maintenance and testing procedures that will help ensure ongoing risk mitigation.

Documenting the plan

IBM clients will benefit from a documented roadmap addressing cloud security strategy. The plan should identify the types of workloads or applications that are candidates for cloud computing and should account for the legal, regulatory and security requirements. IBM will work with clients to plan for compensating controls to mitigate perceived risks, including how to address identity and access management, and how to balance security controls between the cloud provider and the subscriber.

Assessing cloud security with IBM

In addition to developing a strategy for cloud security, IBM can perform a cloud security assessment for public or private cloud offerings. This service can provide helpful due diligence for cloud providers, or help subscribers understand the security posture of their provider's cloud.

The IBM cloud security assessment reviews cloud architecture from a security standpoint, including policies and processes for data access and storage. IBM security experts assess the current state of cloud security against best practices, and against providers' own security objectives. Security requirements and best practices criteria is based on unique characteristics of the subject cloud, including workload, trust level of end users, data protection requirements and more. For example, clouds supporting email will have different security requirements than those supporting electronic Protected Health Information (ePHI).

A gap assessment against security objectives and best practices will reveal strengths and weaknesses of the current security architecture and processes. IBM experts will provide recommendations for improvements and continuous security measures to bridge the gaps. These can include the use of additional network security controls, modifications to existing security policies and procedures, implementation of new identity and access management controls, acquisition of managed security services for offloading critical security management tasks, or any number of other remediation steps.

In addition to a thorough review of the cloud security program, IBM advises steady state technical testing of the cloud's network infrastructure and supporting applications via remote penetration and application testing. This provides a "hacker's eye" view of cloud components and provides insight into how cloud security weaknesses can significantly impact data and information protection.

Why IBM?

To fully benefit from cloud computing, clients must ensure that data, applications and systems are properly secured so that cloud infrastructure won't expose the organization to risk. Cloud computing has the usual requirements of traditional IT security, though it presents an added level of risk because of the external aspects of a cloud model. This can make it more difficult to maintain data integrity and privacy, support data and service availability, and demonstrate compliance.

Assessing the risks associated with cloud computing, such as data integrity, recovery, privacy, and tenant isolation is critical to the adoption of cloud technologies. These risks call for automated end-to-end security with a heavier emphasis on strong isolation, integrity and resiliency in order to provide visibility, control and automation across the cloud computing infrastructure.

IBM helps clients put risk management strategies into action by transforming security from a cost of doing business to a way to improve the business. IBM draws from a broad portfolio of consulting services, software and hardware and managed security services that enable a business-driven approach to securing your cloud computing as well as your physical IT environments.

IBM's capabilities empower you to dynamically monitor and quantify security risks, enabling you to better:

- Understand threats and vulnerabilities in terms of business impact,
- Respond to security events with security controls that optimize business results,
- Prioritize and balance your security investments.

IBM also securely operates its own public clouds, including IBM LotusLive™. IBM continuously invests in research and development of stronger isolation at all levels of the network, server, hypervisor, process and storage infrastructure to support massive multitenancy while mitigating risk.

Through world-class solutions that address risk across all aspects of your business, IBM is able to help you create an intelligent infrastructure that drives down costs, is secure, and is just as dynamic as today's business climate. IBM cloud security solutions and services build on the strong foundation of the IBM security framework to extend benefits from traditional IT environments to cloud computing environments.

For more information

To learn more about the IBM Cloud Security Services, please contact your IBM marketing representative or IBM Business Partner, or visit the following website: **ibm.com**/cloud

Additionally, financing solutions from IBM Global Financing can enable effective cash management, protection from technology obsolescence, improved total cost of ownership and return on investment. Also, our Global Asset Recovery Services help address environmental concerns with new, more energy-efficient solutions. For more information on IBM Global Financing, visit: **ibm.com**/financing

Route 100
Somers, NY 10589 U.S.A.

Produced in the United States of America
November 2010

Please Recycle

SEW03022-USEN-01