Insight in the Cloud

How Cloud Security Assessments Help Businesses Realize Benefits & Reduce Risk

SECURANCE CONSULTING

Introduction

Cloud services offer businesses more agility, flexibility, and efficiency, but they do not eliminate risk or guarantee compliance. Ultimately, the responsibility for compliance and security rests with the business even when the cloud service provider (CSP) offers protection. To safeguard data and reputations, organizations must continue to assess risk, compliance, and liability exposure as they expand into the cloud.

Cloud-based solutions are not inherently less secure than traditional solutions, but the complexity of service agreements and the relationship between internal and external systems makes assessing compliance and security in the cloud challenging.

This should not prohibit businesses from reaching into the cloud to extract the benefits cloud services deliver—including cost efficiency, reduced operating complexity, and new ways for employees to collaborate. These benefits are especially important to small and medium-sized businesses (SMBs), where economies of scale are often more difficult to achieve than they are for large, global enterprises.

This paper provides an overview of cloud services, discusses cloud-specific vulnerabilities, and offers insight on how businesses can assess and mitigate risk in the cloud.

Overview

By 2014, 87% of businesses were operating in the cloud and more than 40% wished they had moved to the cloud sooner. Despite this enthusiasm, many businesses report that they don't have a mature cloud strategy or a clear understanding of cloud vulnerabilities. Before discussing the unique security threats of cloud environments, it's necessary to differentiate between cloud deployment models and the services they offer.

Both the deployment model—public, private, hybrid, or community—and the type of services being delivered—Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as Service (SaaS)—will impact testing and analysis during a cloud security assessment. For instance, some CSPs limit intrusive testing, while others require customers to take full responsibility for security and testing.

Decision makers need to consider how vulnerability is typically managed in each deployment model and what level of security providers offer. Even if a CSP takes responsibility for a portion of IT security, those guarantees must be verified before they are trusted. If the provider is attacked and sensitive information is stolen, customers and regulatory agencies will hold the business accountable, not the CSP.

Cloud Services

Infrastructure as a Service (IaaS)

- Basic computing infrastructure, storage and networking capabilities built on virtual machines.
- Reduces IT administrative effort and hardware and maintenance costs.
- Business controls operating systems and middleware and applications.
- CSP secures virtualization technology and physical hardware.

Platform as a Service (PaaS)

- Environment and platform used by developers to develop and test software.
- Reduces staffing and operating costs, allowing developers to focus solely on development and not maintenance.
- Business must secure deployed applications and, in some cases, hosting environments.
- CSP manages infrastructure.

Software as a Service (SaaS)

- Applications and software developed and deployed by the CSP and accessed by a thin-client interface.
- Reduces complexity while expanding software offerings and availability.
- Business has limited ability to control security.
- CSP must secure applications and infrastructure.

Who holds the responsibility for security in the cloud shifts depending on which services are adopted and which deployment model is utilized. Security for private clouds is managed internally by the organization. Public clouds and hybrid clouds incorporate extra-organizational components, distributing security responsibilities based on architecture and contractual agreements between the organization and the CSP

Cloud solutions can increase risk because of variability among solutions and providers and the likelihood that individuals will move data to the cloud without IT approval. However, most SMBs already utilize cloud solutions and realize the competitive advantages, so delaying cloud adoption unnecessarily prioritizes security concerns over business benefits.

There is no compelling need to approach the cloud timidly or avoid it. Businesses can identify, analyze, and mitigate risks in the cloud to obtain the benefits of increased agility and efficiency while safeguarding data, systems, and intellectual property.

Cloud Deployment Models

Public Cloud

External
Network open for public use
Cost efficient
Easily accessible by non-IT users

Private Cloud

Internal
Accessible by one organization
Major capital and knowledge investment

Hybrid Cloud

Combination of multiple clouds
Access is private but bound to public resources
Cost depends on design

Community Cloud

External
Access is limited to organizations with similar computing needs
Cost is distributed

Balancing Risks & Advantages

New technologies are referred to as “disruptive” for a reason: they alter how people and organizations work, fundamentally transforming behaviors and processes. That degree of change and innovation comes with its own challenges, and many businesses hesitate to advance into the cloud, fearing the costs and consequences won’t be worth it. Here we consider four challenges that stakeholders must weigh when they consider deploying cloud services.

Challenge #1: Doing Nothing

Most businesses are already operating in the cloud and realizing the benefits of cloud solutions—cost efficiency, increased collaboration (between employees, business units, and partners), reduced complexity, and enhanced agility. Clinging to traditional models for delivering IT services can feel safe, but it becomes a disadvantage as competitors become more agile. In actuality, pushing *further* into the cloud is beneficial for many businesses, especially SMBs that can access pay-as-you-go cloud solutions that would be too complex or expensive to deploy and manage within the confines of a traditional IT environment.

74%
businesses surveyed reporting competitive advantages realized with the introduction of cloud services

Five Business Advantages of Cloud Services

1. Expanded collaboration between business units
2. Reduced operational complexity
3. Improved customer service
4. Lower operational costs
5. Increased flexibility & agility

Challenge #2: Rogue End-Users & Shadow IT

Cloud services are readily accessible by businesses and individuals. Employees who rely on cloud services for personal use—like email, file sharing, and software solutions—are likely to seek the same level of flexibility and availability in the work environment. Businesses that reject or severely restrict cloud services inadvertently compel employees to find solutions independently, without going through proper IT channels. The use of these unmanaged shadow IT services heightens the risk of breaches and data loss and erodes compliance.

Challenge #3: Security Beyond the Perimeter

As discussed earlier, CSPs offer different levels of security depending on the deployment model and the services provided. Large enterprises can deploy cost-efficient private cloud solutions, but private clouds are expensive and finding experienced staff is difficult and costly for SMBs.

Small and medium-sized organizations gain more by utilizing public, hybrid or community clouds, while carefully assessing and managing risk. Unfortunately, relying on self-reported security information from CSPs is inadequate. Organizations must thoroughly test all systems or demand comprehensive reports that adhere to industry standards if intrusive testing of CSP systems is prohibited.

Shadow IT — technology systems and services running inside a business network without the approval of an organization's IT department. These solutions heighten risk and increase vulnerability and liability in the environment.

Challenge #4: Compliance

Running afoul of regulatory compliance is a risk whether or not an organization embraces cloud services, but the cloud introduces unique regulatory challenges. Resources are shared between many different organizations in public clouds and data could be stored anywhere in the world, which could force an organization to adhere to additional regulations in the host country.

These compliance issues do not mean that government agencies, healthcare companies, and financial institutions should avoid the cloud. At this point, the risk of not evolving is too great. Instead, organizations that face considerable regulatory constraints should seek qualified partners at the start of any cloud deployment to develop and deploy solutions that enhance agility and maintain compliance.

33%
midsize businesses will be using public cloud services within 5 years

An organization could be subjected to regulatory compliance in another country if a CSP stores data data in that country. Always verify where data will live and how that affects regulatory compliance before you sign up with a CSP.

The Advantage of Insight

Disruptive technologies transform operations, but the old adage that knowledge is power remains true. Security assessments deliver crucial knowledge about cyber defenses and this insight is essential to risk management and compliance.

Technology Evolves But Many Risks Remain

Approximately 90% of the technology breaches in 2014 could have been easily prevented by security assessments and practical risk management. Since cloud computing and traditional IT systems have many threats in common, businesses must inventory, classify, and analyze risks in the cloud as they would conventional infrastructure.

In traditional IT environments, testing cyber defenses often saves money and reputations by uncovering vulnerabilities before hackers exploit them. Thus far, data breaches have occurred less frequently in the cloud, creating a false sense of security. Moving forward, the cloud will attract more attention from hackers, who will shift their focus to follow the data. Organizations that proactively extend digital defenses and risk management to the cloud will be less appealing targets.

Top 5 Cloud Security Threats

1. Data Breaches
2. Data Loss
3. Account Hijacking
4. Insecure Application Program Interfaces (APIs)
5. Denial of Service Attacks

Cloud Security Methodology

There are similarities between traditional IT and cloud security assessments but the latter require specialized knowledge of the technical strengths and vulnerabilities specific to cloud services. Beyond the technical aspects, cloud assessments are complicated by contractual agreements with CSPs. Organizations may be required to take full responsibility for testing or they may face strict limits on testing. Auditors have to analyze the organization's risk management objectives and regulatory requirements alongside restrictions in the provider's service level agreement (SLA).

When intrusive testing is prohibited, organizations should receive reports containing detailed information about risk management and regulatory compliance at the CSP. Those reports must be evaluated and integrated into risk management and compliance planning within the organization. If the SLA does not provide adequate protection, additional layers of security may be necessary to protect data and ensure business continuity.

Further complicating matters, many CSPs rely on contractual limitation of liability clauses that restrict damage claims to a refund of fees paid. In these cases, businesses face substantial costs in the wake of breaches, data losses, or service interruptions. Analyzing business continuity plans, disaster recovery strategies, and incident management should be an integral part of cloud deployments and must be reassessed periodically.

Cloud security assessments require experienced auditors and proven methodologies that factor in all of the technical and regulatory complexities of operating in the cloud. Organizations should look for partners that demonstrate an understanding of cloud services, how they integrate with traditional IT infrastructure, how to measure the impact of SLAs, and how CSP controls affect governance, risk, and compliance.

Experienced Guidance

Cloud security assessments are complicated by the intricacies of service agreements, competing internal and external interests, geographical complexity and the need to balance security risks with business benefits. The Securance Consulting methodology aligns information security best practices, regulatory requirements, and the latest standards of cloud computing to deliver customized solutions that support continuous monitoring and durable security.

Contact Securance Consulting for a detailed description of our cloud security assessment methodology and to discover how our consultants can help your organization evaluate cyber security and mitigate risk.

SECURANCE CONSULTING

Securance Consulting
13904 Monroes Business Park
Tampa, FL 33635

Office: 877.578.0215
Direct: 877.578.0215 x122
Fax: 813.328.4465
contactus@securanceconsulting.com

Sources

http://www.cloudcomputing-news.net/news/2014/apr/08/why-cloud-services-spending-will-exceed-174b-in-2014/
https://hbr.org/resources/pdfs/tools/Verizon_Report_June2014.pdf
http://www.mcafee.com/us/resources/reports/rp-six-trends-security.pdf
http://reports.informationweek.com/abstract/5/11335/Cloud-Computing/Research:-Cloud-Security-and-Risk-Survey.html
http://www.forbes.com/sites/louiscolumbus/2013/07/30/roundup-of-small-medium-business-cloud-computing-forecasts-and-market-estimates-2013/
http://searchsecurity.techtarget.com/news/2240238606/Report-More-than-90-of-2014-data-breaches-could-have-been-prevented
http://www.cpapracticeadvisor.com/news/11362644/80-percent-of-smbs-say-cloud-computing-helps-them-thrive