9 Critical Points to Create Cloud Security

Understanding and Evaluating the Risks of Cloud Computing

By John Molinaro | August 21th, 2013

Whether your company is already using cloud computing or it is contemplating expanding its cloud usage, the creation of a solid cloud security strategy is necessary to support your endeavor. Your customers, employees, shareholders, business partners, and governmental bodies all have the expectation and understanding that working with your organization is a secure venture. The slightest compromise can have detrimental results so it's extremely important that your company identifies the different levels of risk in order to achieve the level of security that best meets business requirements and compliance guidelines.

The task of creating a cloud security strategy can be a struggle since it is not only imperative to identify and address the risks of company stakeholders, but to do so while keeping costs low and complying with resource constraints. Often times, there are conflicting views and needs revolving around the discovered risks. Developing a central governing board to attend to the needs of the various stakeholder groups will result in a holistic approach that satisfies all of the strategy requirements.

When building a security strategy for the cloud, it is necessary to understand the full impact of the risks involved in order to make informed decisions about strategy directions and requirements. Below is a list of 9 critical points to remember when addressing cloud security:

1. Cloud security needs to be approached from a risk management perspective. If your organization has a risk management team or governing body, they must be involved in cloud security planning.

2. Your organization's IT department *must* be involved in the development of a cloud security strategy. While infrastructure, data, and integration services are included in the role of IT, cloud discussions may begin in other departments as SaaS application offerings reach beyond IT. It's vital for IT to be involved as early and often as possible.

3. IT security monitoring has no concrete key performance indicators. Be aware of what *can* be monitored and continuously track these metrics in order to discover new trends.

4. Clearly define the rules, flow, and automation of cloud processes. In an environment with multiple cloud users, it is necessary to identify which users are allowed access to which resources and under what circumstances. In addition, tracking how and when the resources were provisioned as well as who approved them will create a solid activity log to inspect security discrepancies.

5. Education of the user and support staff is essential. Create awareness of security risks by developing internal education programs and guarantee compliance by understanding that the biggest security threats come from within.

6. Seek expert advice while continually reviewing and assessing standards, policies, and systems. Security standards are constantly evolving alongside compliance, regulatory, and legislative policies. It's important to regularly review them and adapt the strategy as necessary.

7. Examine and update your patch management and change management processes. Ensure that your cloud service provider (CSP) is aware and/or contractually obligated to adhere to these specific policies.

8. Review other Information Technology Infrastructure Library (ITIL) processes as well as the systems for backup creation and disaster recovery.

9. Know where your data and backup data lives, and understand how it is managed.

Understanding that data theft and security breaches are huge non-recoverable losses in trust, developing a strong cloud security strategy is imperative to successful businesses and client relationships. While the 9 critical points discussed above represent the most fundamental considerations, it is essential to remember that these considerations themselves are perpetually in a state of change. Constantly re-examining your cloud security strategy will not only result in a more protected system, but one that all of your company stakeholders can trust.

About the Author:

John Molinaro is a career technologist and business leader. Throughout his career, John has blended together business needs and technological innovation, resulting in the creation of numerous industry solutions. For more information, John can be contacted at john.molinaro@sterliteusa.com or 219.629.0662.