Moving Securely to the Cloud

Gain the advantages and avoid the risks

By Steve Weil

The Challenge

Across the world, organizations are adopting cloud-based services to gain the benefits of rapid deployment, scalability, and cost savings. According to a survey by Forrester Research, Inc., fully 79 percent of technology and business decision-makers prioritized upgrading or replacing their legacy systems with cloud technology in 2015.

Yet security worries still prevent many organizations from moving their sensitive data and business functions to the Cloud. With cybersecurity breaches on the rise, executives and boards of directors are increasingly concerned about protecting their organizations' data and information systems, whether they are in or out of the Cloud. C-suite executives are demanding rigorous due diligence & greater security controls—and wondering if it's enough.

The hesitation to fully embrace the Cloud is perpetuated by two common but conflicting myths about its security: one, that the Cloud is secure by default; and two, that the Cloud can never be secure enough for sensitive data and information systems. The reality is that, with proper planning and controls, the Cloud can be secure enough for even sensitive data and information systems.

How can your organization reap the full benefits of the Cloud and avoid potential security risks?

Point B's Approach

Point B's approach to Cloud security is rooted in our impartial perspective. Being independent of third-party providers enables us to create effective solutions for our clients.

In our experience, four fundamental steps are key to making a secure move to the Cloud:

- ✓ Identify which security controls will be managed by your cloud service provider (CSP), and which are your responsibility.
- ✓ Encrypt all data stored in, and sent via, the cloud.
- ✓ Establish formal, documented service-level agreements (SLAs) and contracts with your CSPs.
- ✓ Use CSPs that have undergone third-party cybersecurity audits.

Establish clear controls and responsibilities

Who's in charge of your data security? It's essential to identify and clearly define which security controls are managed by your CSPs, and which are your organization's responsibility.

Organizations should never rely solely on their CSPs to fully secure their data and information systems.

Ultimately, your organization is responsible for securing these valuable assets—wherever they reside.

Because the dividing line between a CSP's cybersecurity responsibilities and those of an organization can be fuzzy, it's important to formally discuss and document these responsibilities with a CSP before signing a contract with them. Verify any assumptions about how a CSP will protect your organization's data and information systems.

Many CSPs, such as Amazon Web Services, have a "shared responsibility model" for security controls. With this model, the CSP takes responsibility for securing the cloud Infrastructure while the customer is responsible for securing the applications and data hosted on that infrastructure. If shared responsibility seems appropriate for your organization, look for CSPs that have formally documented this model. You want to choose a mature organization that clearly understands its security responsibilities.

Encrypt all data being sent and stored

Making a secure move to the Cloud includes ensuring that all data is sent encrypted when it's being uploaded to or downloaded from the Cloud. Also be sure to strongly encrypt all sensitive data (e.g. medical information, financial data) stored in the Cloud.

Strictly limit who is allowed to decrypt sensitive data stored in the Cloud. Never store decryption keys with encrypted data in the Cloud. And do not share your cryptographic keys with your CSP; your organization should have sole control over them. Reduce your risk by documenting and implementing a formal cryptographic key management process that covers the generation of strong cryptographic keys together with their secure distribution and storage.

Spell it out: service-level agreements and contracts

A service-level agreement (SLA) can eliminate gray areas by defining expected levels of service for a CSP, along with the consequences (such as a customer service credit) if such levels are not met.

In addition to standard requirements such as availability and performance, be sure to include cybersecurity-related items, such as the maximum time before a cybersecurity incident at a CSP must be reported. This sets a tone with the CSP and lets them know your organization takes cybersecurity seriously.

Your contract with a CSP should clearly state the security controls and cybersecurity standards that the CSP must maintain (e.g., PCI DSS, HIPAA, FISMA)—along with your right to audit their compliance. It should state that your organization owns the data it has stored with the CSP, and that you have the right to get the data back. It should also give your organization the right to stop using the CSP if it does not meet the requirements of your contract or SLA.

Go with an audit-proven CSP

Choose a CSP who regularly has independent third party assessments of their cybersecurity practices. Third party assessments are usually more rigorous and meaningful than self-assessments. Depending on the nature of your business, good third-party assessments for CSPs include SSAE16, PCI DSS, FedRAMP and CSA STAR. Whenever possible, ask to see the full assessment reports; they contain much useful information about CSP cybersecurity practices.

The Bottom Line

In the end, the Cloud is as secure as your organization and your CSPs make it—together. Choose a mature CSP that has gone through independent audits. Insist on detailed contracts and SLAs. Encrypt your data. And establish clear internal controls and responsibilities. These essential steps will enable your organization to move to the Cloud with confidence.

