Security – your biggest challenge in the Cloud

While the benefits of migrating to the Cloud in terms of reducing operating costs and technology complexity have been well documented, redrawing an organization's security policy in preparation is a more drawn out exercise, says Sachin Bhardwaj, Director Marketing & Business Development, eHosting DataFort.

The challenges of securing an organization's data assets in the Cloud remains the primary inhibitor towards migrating to the Cloud. While many organizations have adopted a Cloud-first approach, many are still reluctant to embark on this journey. It is not enough to start checking boxes as done, when initiating a Cloud migration exercise. The big picture of how to get a return on investment includes redrawing an organization data security policy to include its Cloud assets and how to manage its Cloud Services Provider (CSP).

Organizations embarking on a Cloud migration journey need to apply due diligence to assess the levels of security inbuilt within their chosen CSP. Expect to see at least one of these compliance specifications stated including ISO 27001, PCI-DSS, CSA-STAR, HIPAA, amongst others. Asking the CSP to formally disclose the level of risk and level of compliance through a questionnaire, is again a common practice, for an organization's legal and security departments.

Spending time on getting these responses, evaluating them, and moving to a high level of transparency in terms of the security preparedness of the CSP, is a commonly practiced way forward for the end user organization. Looking closely at the responses from the CSP will help answer questions about the inbuilt levels of security.

Spending time and aggregating these responses will help to build a suitable data security policy, applicable to an organization's Cloud assets. Moreover, an organization's core IT team must always be involved in any Cloud migration exercise from the early stages. The biggest mistake may be to move into a CSP's environment that is not as securely protected as the organization's on-premises environment.

When migrating workloads from on-premises to the Cloud, the robustness of the organization's data classification gets tested. Not all data needs to be moved from an onsite-premise, with a listed compliance requirement, into a Cloud environment. In other words, data classification policies applied onsite also need to be applicable in the Cloud, in terms of exclusion and inclusion of data.

Another fundamental change from on-premises data management to Cloud-based data management, is ownership of responsibility. End user organizations will typically find that once their data has been moved to a Cloud environment and if managed by the CSP, the skills required to perform IT management and administration roles will become redundant. This will require a new portfolio of skills by the end user organization, as they will be involved more in monitoring and managing the operations of the CSP.

The most critical part of the relationship with a CSP, is where the hard line between the two sides is blurred and without clarity on the exact nature of responsibility from both sides. The end user organization needs to work decisively towards redefining and clarifying any such fuzzy areas for lack of security compliance and data integrity within the CSP.

The more effort that goes into establishing clarity on the roles played by the CSP and the end user organization, especially around data integrity and data protection, the more likely that the relationship will progress from short term implementation to long term stability.