Corporate data in the cloud

Three’s a cloud

Businesses continue to plunge into cloud computing with gusto, but are they fully aware of the challenges surrounding the number of parties involved? The element of risk and governance changes heavily depending upon who is in control – you, your provider or a third-party. Who’s in charge?

There are many circumstances that can arise with the result of your data falling into the hands of a third-party provider, such as vendor acquisitions, mergers, or outsourcing to SaaS. The risks surrounding data in the cloud will rise and fall significantly if your business is not on top of the regulations regarding data ownership.

It is vital for your business to be fully aware of the potential risks, and also what the possibilities are of a third party becoming involved and perhaps withholding your data.

Customers must ask themselves some important questions – will a third party follow the same security regulations and guidelines as my chosen vendor? What's the policy toward retracting my data from the third-party cloud? Do I have a business continuity plan if there is an issue with the third party? How much, if anything, do I know about this third party?

"Generally, companies signing up to cloud solutions would be expected to do extensive research before investing in that solution and it is the CIO's responsibility to make sure that sufficient due diligence is done to have cloud as part of their infrastructure plans. Nevertheless, businesses need to be aware of user access privileges and what sort of access they are granting a third-party cloud provider. Questions they need to ask are, 'Who at the back end has access to my data?' and, 'If they do have access, how often and why?'" says Nassir Nauthoa, General Manager, Intel GCC.

Joe Fagan, Cloud Sales Director, Seagate EMEA, believes it's a little bit more complicated than this: "Few people really understand all the legislation surrounding third-party cloud services because the legislation itself has not yet caught up with reality."

"In fact, in most territories, there are conflicting pieces of legislation regarding retention and disposal of certain types of data. For the time being, best practice is to be able to demonstrate that reasonable efforts are being made to comply with the most relevant industry sector and geographic legislation that applies. The cloud service provider is normally aware of the applicable legislation and should consult partners in this regard."

According to the experts, there are a multitude of **LAWS** covering different areas that need to be considered when moving onto the cloud.

> “Organisations that want to manage information have to define data strategy and clear visibility into the information value chain. Defining what 'data ownership' means is critical to identify stakeholders, align expectations and deliver value from data in the cloud.”

Joe Fagan, Cloud Sales Director, Seagate EMEA

Who's in control?

Critically, once your contract agreement has been signed and your data is in the cloud, it's important to understand who has ownership and responsibility for it. Too often, companies get into service agreements with cloud providers without understanding the regulations surrounding such issues.

"One of the main challenges of adopting cloud solutions in the Middle East is that while there are regulations in place, they are confusing, inconsistent and in some cases contradictory. Lack of a clear regulatory environment is slowing down cloud adoption in the region," says Kevin Harris, Enterprise Technologist, Cloud Computing, Dell Emerging Markets.

"There is almost always confusion regarding the regulations involving third-party cloud services," agrees Geoff Webb, Director of Solution Marketing, NetIQ.

"This is because the multi-national nature of many cloud services makes it very difficult to get a clear picture of what regulations apply, and how. For example, organisations should consider if data stored in a U.S.-based service provider is affected by local laws – and how would that be different if the data centre was located in Europe, for example. The nature of cloud is that often customers do not see the exact details of how services are delivered, but this lack of clarity can also be a cause of problems, too."

Ash Ashutosh, CEO and Founder, Actifio, also believes that extensive research is critical. However, he says that cloud suppliers themselves should be the party doing investigation into regulations, suggesting that it can also double as a sufficient guide for customers.

However, regardless of these arguments, someone has to take full responsibility of that data – but who?

Corporate data in the cloud

"In a multi-tenant environment, cloud service providers bear a large responsibility for the security and access rights of the data held in their systems," says Nauthoa.

"This obviously has to be a central tenet of their value proposition to would-be users of their services. It's also incumbent for customers to ensure that they work closely with service providers to ensure that their data integrity is being met through use of best-in-class technologies as part of their SLAs with these companies," he adds.

Rajesh Abraham, Head of Product Development, eHosting DataFort, says, "There are two key issues, which are data security and reliability. This is also a reason why users are slower to adopt cloud storage. Enterprises today focus on different aspects of data in order to protect the environment.

"Organisations that want to manage information have to define data strategy and clear visibility into the information value chain. Defining what 'data ownership' means is critical to identify stakeholders, align expectations and deliver value from data in the cloud," Abraham adds.

Rajesh Ganesan, Director of Product Management, ManageEngine, takes the firm standpoint that single ownership is the wrong way to go.

"Once corporate data is in the cloud, a single hand being fully responsible is not the right model. 'Trust but verify' works better in all scenarios, so both the business and the cloud provider are equally responsible for the corporate data in the cloud.

Securing data access

Questions of data responsibility and ownership surely spark the issue of governance and data control. Though all parties must be involved in the due diligence, not every part will end up pleased, as Seagate's Fagan explains.

"There are constantly new ways to reduce the chance of data disclosure. Physical access can be made even more secure, and the technology exists to reduce cyber access to someone else's data. The trade-off is always the inconvenience to the legitimate consumer of the data. In that sense, it's really a question for the corporate customer to decide."

Webb raises the topic of mobility and BYOD, and how employees wanting to embrace this trend need to be properly considered if the company wishes to move into the cloud.

"To minimise the risks of moving into the cloud, businesses need to be clear on the use of 'identity' to control access to cloud-based applications and services," he says.

"This is especially true when these services are accessed via mobile devices which are owned by the employee, which is increasingly the case. By thinking carefully about the role of identity and access controls, each employee's access rights can be more easily set to the appropriate level and therefore IT can help prevent sensitive information from being accessed in an insecure way."

BYOD is a large concern for companies wishing to move onto the cloud.

Nassir Nauthoa, General Manager, Intel GCC

If worse comes to worst

Unforeseen circumstances may appear for enterprises that will have them worried about their cloud-based data. This could then quickly lead to the need to remove and retain corporate or sensitive data from the cloud. Contractual agreements will have policies in place surrounding this type of action. Webb says that this situation can be very sensitive.

"Recovery of data from a cloud service is always a sensitive subject and must be addressed in the service level agreements and contract," he stresses.

"The real risk is that the service provider may not adequately destroy data on systems (and in back-ups and images of virtual machines) and therefore the data continues to represent a risk to the organisation long after they have terminated their relationship with the provider."

Third-party agreements in cloud contracts can pose obvious complications, as outlined here. As the experts have outlined, a fully fledged investigation into all parties involved is highly recommended. ■