**YOU CAN STRENGTHEN SECURITY WITH THE CLOUD**

CIOs unfamiliar with cloud computing are concerned over how to maintain IT security once their infrastructure is off-premises. Physical access to servers running their virtualized infrastructure, multiple forms of data security, and the ability to pass a variety of regulatory compliance audits are all justifiable concerns that need to be addressed before companies can safely embrace cloud computing. Fortunately, competitive cloud providers can provide solutions to address all these problems. Don’t be satisfied with a cloud provider unless it can provide at least the same level of physical and data security as your current data center, and preferably exceed those levels. Start by choosing only public cloud providers with:

* **Demonstrated physical security.** A competitive cloud provider will be able to demonstrate that its data centers are physically secure – preferably with regular audits that comply to ISO 27001 standards. A competitive cloud provider’s points of presence should be state-of-the-art data center facilities that employ the very latest in access control and data protection. Your IT staff should be able to quickly build a list of physical security and data protection requirements, and your cloud provider needs to meet those.
* **Demonstrated experience in IT security.** Long and demonstrable experience in IT and data security is paramount, and it should go beyond just hardware security at the cloud provider’s sites, extending to software security up to and including full volume data encryption, granular server and data access control, and detailed audit logs. You should be able to protect data access from anyone, including the cloud provider’s own on-site technical staff. And finally, any enterprise-capable cloud provider should make sure that your data won’t be accessed by cloud IT staff or mined for commercial purposes by other customers.

Those building private cloud infrastructures have fewer security worries, since infrastructure is still on-premises. But private clouds do have security issues of their own that need to be addressed:

* **Identity management.** This is probably the most important private cloud security concern. Giving users the ability to access IT resources directly via self-service portals makes identity management more important than ever. Your IT infrastructure must implement an identity management solution that’s compatible with your self-service portal and with your cloud provider’s identity management platform if you intend to leverage a public cloud model.
* **Regulatory audits.** While private clouds are located on-premises, it’s still a new model of enterprise computing. Make sure your regulatory requirements are being met in this model by running test audits – if a public or hosted private cloud model is your eventual goal, your public cloud provider can be an excellent resource here. In most cases, you’ll find the provider has experience dealing with your specific audit requirements.

Next to security concerns, some CIOs are also worried about losing control of their IT operation – day-to-day management, physical control and data sovereignty are important concerns. But a competitive cloud computing solution should enhance all these facets of your IT operation, not endanger them. Today’s IT management toolkits can span the gamut between on- and off-premise cloud computing elements, managing both as a cohesive whole and actually increasing response times and application performance. Cloud computing providers should be able to provide at least the same level of physical and data security as your current data center, and in most cases exceed those levels. Start the conversation with your cloud computing provider today, and get the answers to these questions. Then use them to build a cloud migration plan that’s right for your organization.

**Getting started.** Talk to your IT security officers and make sure an accurate and detailed list of requirements is available. Audit your identity management system and make sure it fulfills your needs now and in both a private and public or hosted private cloud computing model. Work with your cloud provider to develop a detailed security policy that’s reflected in your SLA.