Private and Public Clouds: Do I Need to Benchmark?

By Taiye Lambo
November 2012

Cloud computing has fundamentally changed the way organizations around the globe approach the utilization and implementation of technology. In the old model, organizations were forced to purchase, manage, and troubleshoot hardware and software in order to carry on essential aspects of their business. This was clearly not the most efficient use of resources, but there was no practical alternative. Today, however, there are enticing and valuable options that utilize cloud computing to varying extents. The cloud helps to simplify and consolidate processes, increase scalability and flexibility, and save money. With the cloud, companies can focus on their core line of business instead of devoting precious dollars and manpower to information technology. This appeals to CIOs, CISOs, and CFOs as well. For example, eFortresses is 100% cloud based: instead of using dedicated servers, we operate in the cloud. Almost all of our business processes are managed through the cloud: email through Microsoft Office 365, accounting and financial reporting through Quickbooks Online, telephones and faxes through VoIP, etc.

However, there is an important distinction to be made between public and private clouds. For example, an organization running a software application on virtual servers within their own data center is most likely utilizing a private cloud, whereas one utilizing a service like Dropbox (which allows for online data storage) is an example of public cloud use. All too often, even CISOs fail to distinguish between the relative pros and cons of private and public clouds. The old model of servers and software physically installed in a brick and mortar office forms one end of a continuum, with a public cloud app like Dropbox representing the opposing end. The private cloud falls somewhere in between these two. The major differences between them are in management and ownership. For example, consider the case of a healthcare company where customers log-in to an online portal to manage their care. This portal would contain very important electronic protected health information (ePHI) that needs to be accessible, yet secure. A private cloud would have the management of the portal done in-house and the content stored in their own data center. A public cloud model would host the data on an Amazon, Microsoft or Rackspace cloud service, with these firms dedicated to management and security of the content. As such, private and public clouds differ primarily on management of data and who owns the actual infrastructure.

After making the decision to utilize cloud technology, there are a variety of concerns that must be addressed. As previously mentioned, cost and efficiency are major drivers of cloud adoption, but there are other drivers prompting adoption, and important security concerns. Based on a company's industry, clients, regulation, data sensitivity, existing infrastructure, strategic considerations, and information technology demands, CIOs must strike the appropriate balance between keeping technology on the ground or in the cloud, so to speak. Without accurate and reliable information, it is hard to determine the actual pros

and cons of making a switch from public to private or vice versa. And it is often difficult to tell after such a switch has been made whether it improved the level of security. Although many people can lecture about whether public or private clouds are *generally* more or less safe and secure, that may not really matter to a CIO, CFO or CEO. What matters to them is whether your private cloud is *specifically* more or less safe and secure than the particular public cloud service provider (CSP) you are considering.

How many organizations who are considering using the cloud, or have switched from private to public clouds, can truly answer whether the CSP has the same level of security, compliance, and their maturity as their own IT infrastructure? Most can neither paint a detailed picture of their current state, nor that of the potential CSPs, and therefore cannot say much about the potential security tradeoffs entailed in a switch. It seems in many ways like an apples-to-oranges comparison. What is needed is a benchmark: an objective measure that will help gauge an organization's current security profile and allow transparent and insightful comparisons to a CSP's security profile. It would allow CIOs and CISOs to make a more informed decision about whether it is safe and secure to move to an external cloud service provider. There are a host of certifications (like ISO 27001, SAS 70 Type I and II, SSAE16, ISAE3402 and SOC 1, 2, and 3), however none of these are specifically designed for cloud security, and maturity level and scope of implementation are hardly communicated clearly by CSPs.

When customers approach a bank for a home loan, they are asked to provide objective evidence of their financial trust worthiness. The bank will use a credit score, obtained from a Credit Agency, which allows the bank to determine their credit worthiness and make an informed risk-based business decision. What we need in the world of cloud computing is a similar trust worthiness score for cloud security: an objective measure that can allow CIOs and CISOs to benchmark their current security state with that of CSPs. Without this, it is impossible to make an apples-to-apples comparison, leaving key decision makers in the dark. So to answer the original question, do you need to benchmark? Yes, absolutely. But without a proper and objective measure of security risk levels, this is a major challenge for CIOs and CISOs to overcome. It may perhaps be the largest question mark in the decision to embrace cloud computing, which prevents decision makers from reducing their risk and promotes a lack of due diligence. In future articles, we will begin to chart a reasonable path forward to addressing this major concern.

About the Author: Taiye Lambo is a seasoned entrepreneur with Global Information Security and Governance, Risk Management and Compliance expertise who is currently focused on Cloud Computing. He is the Founder of USA based CloudeAssurance, Inc., eFortresses, Inc., the Holistic Information Security Practitioner Institute (HISPI) and the UK Chapter of the Honeynet Project and can be contacted via E-mail (tlambo@eFortresses.com), LinkedIn (http://www.linkedin.com/in/taiyelambo) or Website (www.CloudeAssurance.com).