Why You Need a Cloud Rating Score

By Taiye Lambo

January 2012

One of the most significant challenges facing managers of information technology (IT) and organizational executives is navigating the play of disruptive technologies. Often, new processes emerge not as incremental improvements to current ways of working, but as fundamental shifts. These new technologies challenge the established business models and offer the promise of a better way. Within the past decade, the most significant disruptive technology to emerge is cloud computing.

According to forecasts by the International Data Corporation, cloud spending will account for 25% of this year's annual IT expenditure growth and nearly a third of the growth next year. It offers a host of important benefits: decreased expenses, improved efficiency, greater scalability, and others. Yet the cloud is not without its own challenges and costs, many of which are hidden. CIOs and CISOs making decisions on how to adopt cloud technology often do so with rather limited, and often incorrect, information. In this article, we will explore the phenomenon of cloud computing and learn how to responsibly and strategically manage its risks in order to achieve the substantial benefits of adoption.

The Promises and Challenges of the Cloud

The appeal of the cloud is not difficult to comprehend. For instance, imagine you are running the IT department at a busy metropolitan hospital. Each day hundreds of patients walk in and out of your doors, leaving behind thousands of pieces of data: medical history, immunization status, test results, billing information, x-ray images, and other personal information. And many of these patients regularly visit doctors outside of your hospital's four walls – the data from these visits may be crucial for your organization to achieve its mission. This is not the sort of environment where paper records would suffice. Consider then the promise of leveraging the cloud to centralize and manage all the patient information across the many different Health Information Exchanges (HIE), healthcare payers, service providers, and the National Health Information Network. It would seem like a miracle solution. In many ways, it is.

The cloud serves to simplify processes, allowing your organization to focus less on managing data over expensive IT infrastructures and instead concentrate on your direct line of business. In addition to promoting a better allocation of your organization's resources, cost savings from using the cloud can be quite significant. Cloud computing also allows a greater degree of scalability: instead of purchasing costly server space or bandwidth based on projected future growth, organizations can add or remove capacity in real-time to accommodate fluctuations in demand. Unlike in-house IT, cloud computing is able to spread loads over many users, which brings hardware and software utilization closer to 80% - often nearly double the rate of in-house IT. The cloud also provides flexibility of managing virtual servers and the marketplace provides the ability to switch service providers rather than fix institutional problems in internal IT organizations.

The benefits to the cloud are, no doubt, numerous and quite enticing. However, what about risks? Only a month ago, a hospital in Georgia experienced a major security incident. It prevented them from accessing any of their patients' electronic health records. Emergency room and trauma patients had to be diverted to other hospitals. Treatments were delayed. Lives were risked. The hospital was reduced to paper and pencil methods. Put yourself back in the position of the hospital CIO. Imagine the questions that would be asked of you: "How could you let this happen?" or "What was your contingency plan?" or "What steps did you take to ensure data safety and security?" Many (if not most) CIOs and CISOs would have few compelling answers to such questions.

The truth is that in many ways cloud security is still a bit like the Wild West. There are many competing security certifications and many cloud services are yet to achieve any of these certifications. For example, it may shock you to know that at the time of this article's writing, a popular cloud service like Google Apps is not yet ISO 27001 certified; especially because ISO 27001 is generally acknowledged as the most comprehensive and globally accepted information security certification. With the rise of cybercrime, major Global 1000 companies, Fortune 500 firms, and government agencies have experienced major security breaches. Even the White House staff had their Gmail accounts hacked in a targeted attack, possibly by a foreign government. This type of cloud related incident should serve as a wakeup call to cloud service customers – consumers and businesses alike.

The Three Elements of Security

How can we better prepare to address the challenges inherent in cloud computing? Perhaps the first step is education. One of the clearest models to understand security concerns is the well-known C-I-A Triad. It addresses the Confidentiality, Integrity and Availability of information as diverse as: patient records, customer credit card numbers, internal documents, email messages, trade secrets, national secrets, and more. Confidentiality essentially means that sensitive information is protected from unauthorized access. This includes both from the outside and internally, when internal users have unnecessary access to sensitive information. Integrity is about both protecting data from malicious modification and deletion and allowing for ways to undo any unintentional corruption of the data caused by authorized users. Availability ensures that the appropriate individuals have access to the data when needed.

What we see here is that key concerns such as confidentiality and availability often stand in opposition to each other. The more that confidentiality of data is ensured, the less available they are, which slows down your organization's processes. Likewise, the more that availability of data is enabled, the less confidential they are, thereby increasing the risk of security breaches. The case of Bradley Manning and WikiLeaks demonstrates this balancing act clearly: military personnel need access to information, but if they are given too much access, they can abuse that same access to sensitive information.

All Clouds are Not Created Equal

Knowing the three important elements of security, we now turn to Cloud Service Providers (CSPs). How can we understand the security protections offered by the broad array of various providers? And most importantly, how can IT managers and executives decide between competing offers based on their organizations' strategic interests?

The answer is not a simple one, but we can begin to outline four important steps in the right direction:

1. *Quality of Certifications*
   Perhaps the first question one should ask of a potential CSP is about their third-party certifications. Although there are no available internationally accepted cloud-specific certification standards yet, pending the release of the cloud-specific ISO 27017 certification standard, ISO 27001 (Salesforce.com, Amazon Web Services, Microsoft Office 365 and Microsoft Windows Azure) remains the industry gold standard. Other less globally accepted certifications include SAS-70 (Google Apps, Microsoft Online and Rackspace) and the relatively new FedRAMP.

2. *Scope of Certifications*
   However, the listed certifications are the first and not the last question IT managers must ask. Keep in mind that the scope of the certification is equally important. Are all CSP locations and infrastructure certified? Are all services being offered certified, or merely those in the CPS's higher end? Certificates do little good unless they cover the full extent of the actual services your organization will use.

3. *Security Maturity Level*
   There are also human elements in addition to the technical ones. Consider the maturity level of the CSPs security program. Does your CSP have processes to prevent or reduce human error? Surprisingly, many CSPs do not even incorporate techniques to properly measure controls effectiveness to ensure continual improvement. Carnegie Mellon's Capability Maturity Model Integration (CMMI) is such a process-oriented technique aimed at assessing and managing risk to ensure continual improvement. Without methods to ensure a high maturity level, individuals within CSPs could bypass processes that increase the risk associated with cloud computing. It would be akin to downloading anti-virus software for your computer, but forgetting to update it to detect and protect against the latest malware.

4. *History of Breaches*
   The fourth question managers ought to ask a CSP is about their history of security breaches. When was the last time they experienced a security breach? What kind of data was accessed? How were clients affected? What have they done since then to prevent future breaches? These inquiries are among the most important that a CIO or CISO can ask a potential CSP.

The Need for an Independent Rating Score

We can see then that cloud computing is the future: it simplifies processes, cuts costs, and provides scalability. The great challenge facing managers of IT and executives is how to best bring the cloud's power to their organization. A whole host of different CSPs exist with different products and services, certified to different standards, extending to varying scopes, and working at different maturity levels. These significant discrepancies make comparisons between various cloud services nearly impossible. How can IT managers and executives manage security risk if they have no accurate measure of each CSP's risk level?

In order to make the best decisions, CIOs and CISOs must have the right information. Especially given the very real threat of class-action lawsuits, regulatory fines, and loss of reputation associated with a security breach. Security breaches at for-profit organizations can impact important bottom-line concerns such as customer attrition and dropping stock prices. In the wake of the American Recovery Act of 2009, the Department of Health and Human services has significantly increased the periodic and random security audits of HIPAA covered entities and business associates, even if there have been no complains or problems reported. Along with the audits come increasingly substantial fines for noncompliance. New regulations include mandatory fines for willful negligence that begin at $10,000 minimum.

As the founder of the CloudeAssurance Rating System Platform, my mission is to help IT managers and executives avoid making costly mistakes in their adoption of cloud computing. CloudeAssurance is the industry's first truly risk-intelligent rating and continuous monitoring system. The CloudeAssurance platform provides a provisional and validated score by consolidating all of the important cloud assurance metrics such as the CSPs adoption of internationally accepted best practices and standards, scope of certifications, maturity levels, Measurement against the Top 20 mitigating controls based on past security breaches, and even industry-specific compliance requirements like PCI-DSS, FedRAMP and HIPAA.

With this score, CIOs and CISOs can feel confident that their cloud computing services are safe, secure, and aligned with their organization's strategic interests. The goal is to keep underperforming CSPs on their toes and allow the most secure CSPs to differentiate themselves and clearly communicate their value to their customers and prospects. For the first time, you can get a single score that weighs all the relevant and available pieces of data. So remember, before you pick a CSP, ask them for their CloudeAssurance score.

This one question could make all the difference between safely and securely adopting cloud computing and ending up as the next poster child for high profile security breaches.

About the Author: Taiye Lambo is a seasoned entrepreneur with Global Information Security and Governance, Risk Management and Compliance expertise with a focus 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).