Corby: Don’t Let the Cloud Catch You Crying

Posted on SecureWorld Post - March 21, 2012

It seems that every decade or so has its new vision for IT services. In the past we’ve chanted mantras such as “virtual machines”, “distributed processing”, “client server”, “thin/thick client” and “web-enabled architecture”. The thought for today’s meditation is “cloud computing”. It may be known as Software-as-a-service (“SaaS”), Infrastructure-as-a-service (“IaaS”), or Whatever-as-a-service (“WaaS”), but the concept is the same: you are not in complete control of all the computer equipment or operating system. So what does that mean for security in your organization? Without going into technical details, configurations and parameter settings, here are a few common sense ideas that will help you plan for cloud services while still retaining sound security practices.

The first issue to address is that you don’t have any hands on access to the cloud equipment. One of the most highly marketed benefits of cloud services is that the expensive and vulnerable electronics are owned and operated by someone else. This, as with many of the cloud service benefits, is both good and bad news. The good news is that you are relieved of the need to size, configure, find capital, select and implement expensive electronics. This expense is shared with your other cloud “neighbors”. You may also be able to avoid the staffing required to keep system programmers, data center operations specialists and highly trained specialists of all sorts. Those skills are also shared with other cloud users.

On the other hand, without these skills and without the ability to make infrastructure changes, you may be stuck with a configuration that doesn’t work as well as it could if you owned it and configured it yourself. To avoid costly delays in implementation and frustrating performance problems, do some advance planning with your cloud provider. See if they have other customers using the software products you are using. Find out from your software vendor (if you use acquired software rather than custom developed programs) if they have had experiences with cloud solutions provides that can help provide direction. Security is about availability, and if the solution doesn’t work or works poorly, it can’t be available when needed. Extensive advance planning can help avoid unexpected issues when it comes time to turn the switch and begin the cloud operation.

The second issue to deal with is that you have put all your critical digital assets in the cloud and may have lost the ability to see and depend on your data and program file backup and restoration procedures. There are three concerns for you to manage: Is the backup being done reliably and according to your prescribed schedule? Does the backup process preserve the data

confidentiality, especially for regulated personal information? Can you find and restore selected files without incurring outrageous costs and spending excessive time searching through offsite archives?

Two key points to keep in mind to minimize the potential for these consequences:

> 1) Make sure you know what you expect the cloud provider to do with your digital repository. Define what files or data elements require special handling with proper storage and retention logs. Monitor those logs (either electronically or in person), and verify that all backup processes have run successfully.
>
> 2) Be sure that the contract provides for you and any third party you authorize to audit the data handling, backup and restore process at least annually, and that any deficiencies are addressed to your satisfaction in a timely manner.

Like I said: Secure implementation of the cloud is not rocket science, but it does require diligent verification, a solid contract, and a clear vision of what you can and should expect from your provider. Armed with these high-level pieces of advice, hopefully you will be better prepared for a rainy day.

Michael Corby, CISSP, CCP, CBCP PMP
Vice President
Risk Solutions International LLC
877-774-1900
www.rsi-llc.com