CITADEL
INFORMATION GROUP, INC.

Eight Security Concerns Before Jumping Into the Cloud

Hypothesis 1: Over the next 3 – 5 years increasing numbers of mid-market and smaller companies will find it makes great business sense to embrace various Cloud solutions, including Salesforce, Exchange and other applications, file servers in the Cloud like Amazon and iCloud, and complete private cloud solutions.

Hypothesis 2: Over the next 3 – 5 years, the epidemic in cybercrime will continue and worsen. Mid-market and smaller companies will see extensive losses of money and productivity as a result. This will tend to drive mid-market and smaller companies towards the Cloud as — all other thing being equal – Cloud providers should be better able to commit necessary talent and resources to security than can organizations for whom IT and information security are not core competences. On the other hand, organizations will have to ensure that in going to the Cloud, they are not jumping into the "abyss of information (in)security."

Eight Security Concerns

Portability: How easy / hard is it to move applications and associated data between one cloud provider and another, or between public and private cloud environments?

Multi-Tenant Security: What steps does the cloud provider take to keep one tenant's sensitive information separate from other tenants? What assurance can the Cloud provider give that sensitive information is kept private? Has there been independent security testing?

Secure Access and Authentication: Is access restricted to a VPN? Are one-time passwords or other 'tokens' supported? How strong is the Cloud provider's authentication mechanism? Is authentication checked at the back-end or only at the client? Has there been independent security testing?

Reliability and Resiliency: What is the ability of the Cloud to provide availability in the face of catastrophic failure of individual components and facilities? At issue is everything from testing backups, the presence of hot sites at remote locations, strategies for countering DDoS attacks, incident response planning, business continuity planning, plan testing, staff training.

Information Security Management: Does the Cloud provider maintain the Cloud environment in accordance with formal documented information security policies and standards? Were these policies and standards developed in accordance with ISO, NIST and other recommended security practices? What special information security certifications do Cloud provider personnel have? CISSP? CISM? Are personnel active in organizations like the Cloud Security Alliance (CSA), Open Web Application Security Project (OWASP) and the Information Systems Security Association (ISSA)?

Compliance with Information Security Laws, Regulations and Third-Party Agreements: Does the Cloud provider meet HIPAA, PCI DSS and other information security and privacy regulations

and requirements? Does the Cloud provider monitor system security activity as required by these standards? [This is different from performance monitoring.] How able is the Cloud provider to support breach disclosure needs or eDiscovery requests?

Encryption at rest: Is your information on the Cloud encrypted? What algorithm is used? How long are keys? Who has keys? How are keys stored and managed? What happens if you lose your keys?

Your Own Information Security Responsibility: *If you collect sensitive information, you are responsible for its security.* Do you have contractual assurance from the Cloud provider that it will secure your information in accordance with your needs to secure it? Has the Cloud provider given you an independent 3rd-Party assessment? [SAS-70 Type 2 is NOT adequate as an information security assessment. You want at a minimum an assessment against HIPAA, PCI-DSS, ISO 27001,02 etc.] Has the Cloud provider clarified exactly what security it is taking responsibility for and what residual responsibility you have? Does the Cloud provider provide information security guidance to help you effectively manage your security responsibilities? Have you discussed cyber security with your attorney; your insurance broker?

The last word goes to Howard Miller, my friend and colleague at L/B/W Insurance & Financial Services in Valencia, CA: *"Maybe the Cloud isn't as solid as we think."*

Reprinted from our blog: www.Citadel-information.com/blog