Risks Associated With Hosting Data in the Cloud

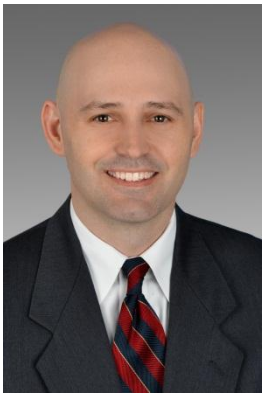
By Brian Von Hatten

Scott & Scott's attorneys are often asked about the legal and compliance risks associated with hosted applications or data in the public Cloud. Depending on the industry, this seemingly transparent choice of where a company hosts its data may actually present significant risks. Given the nature of how data is stored in the Cloud, companies potentially have less control over the management, storage, and access of their data, which results in increased compliance and legal liability challenges.

For example, the financial and health care industries are heavily regulated industries, particularly with respect to the handling of sensitive customer information, often referred to as personally identifiable information ("PII"). For these industries, the Health Insurance Portability and Accountability Act ("HIPAA") and the Gramm Leach Bliley Act ("GLBA") are two main sources of regulatory concern. These statutes have affirmative duties for companies after a security breach has potentially allowed unauthorized access to a customer's PII. Other statutory requirements include taking measures for protecting customers' PII, various opt-out provisions concerning disclosures to affiliates, and ensuring compliance by third-party service providers. Although there is typically not a private cause of action, there can be significant financial risks from non-compliance. Many regulatory agencies have discretion to impose significant monetary fines for failure to comply.

Additionally, there are several other organizations whose comments, interpretations, and recommendations concerning information governance are widely accepted. Such organizations include the Federal Financial Institutions Examination Council ("FFIEC"), National Institute of Standards and Technology ("NIST"), the Payment Card Industry Data Security Standard ("PCI DSS"), and the Cloud Security Alliance ("CSA"). These organizations have drafted handbooks, standards, and "best practices" which would be relevant in quantifying risk factors associated with hosting PII in the cloud, negotiations with the Cloud services provider, and ongoing management of Cloud service provider.

When considering placing sensitive information or PII in the public Cloud, a company should perform considerable due diligence before doing so. Such diligence includes but is not limited to reviewing any specific regulatory requirements for its industry such as HIPAA and GLBA, and ensuring compliance with the recommendations provided by the FFIEC, NIST, and CSA, among others.



About the author Brian Von Hatten:

Brian represents many large and mid-market organizations on matters related to transactions, software licensing, and disputes. Brian's focus includes substantial attention to complex information technology issues for companies of all sizes.

Get in touch: bvonhatten@scottandscottllp.com | 800.596.6176