LOCKE LORD® QUICKStudy
Intellectual Property Practice
July 17, 2012

Financial Regulators Issue Statement Regarding Cloud Security

By: Bart Huffman, Tammy Ward Woffenden, Jennifer Rangel

Last week, the Federal Financial Institutions Examination Council (FFIEC) issued a statement regarding key risk considerations associated with outsourced cloud computing. This is one of the first pieces of federal guidance on the use of the cloud. Moreover, because federal regulation has been at the forefront of data security regulation and best practices in recent decades, businesses that are not financial institutions should also consider the advice.

The FFIEC recognizes that outsourcing data storage and/or information services technology to a cloud vendor can be beneficial due to cost reduction, flexibility, scalability, improved load balancing, and speed. However, the FFIEC warns that financial institutions should ensure that their data remains properly protected and that access is appropriately restricted. The FFIEC's statement discusses the following key elements.

Due Diligence

A financial institution's board of directors and management are generally expected to ensure that outsourcing is conducted in a safe and sound manner that complies with applicable law. With that in mind, the FFIEC advises financial institutions to consider the following types of issues:

- What kind of data will be placed in the cloud? How sensitive is it and what encryption and other controls are necessary for particular categories of data?
- Will resources be shared with other cloud clients? For example, will the institution's data be transmitted over the same networks and stored or processed on servers that are used by other clients?
- What type of access does the vendor have and need to have, and can encryption be used to address any related concerns?
- Are the vendor's disaster recovery and business continuity plans adequate and well-documented?

Vendor Management

Financial institutions should select vendors that are familiar with the financial industry and that can satisfy related regulatory requirements for safeguarding sensitive data. The institutions need to ensure that, as requirements change, vendors can and do make appropriate adjustments. Vendor management is an ongoing activity that lasts up to and sometimes even beyond termination.

Audit

An institution's policies and practices may require adjustments to provide acceptable IT audit coverage of outsourced cloud computing and it may be necessary to increase the number of dedicated audit personnel and provide additional training to audit staff.

Information Security

Information security policies, standards, and practices may need to be revised to incorporate activities related to cloud storage and other cloud services. An appropriate amount of ongoing monitoring is necessary to sufficiently assure that effective controls are maintained.

As the FFIEC observes, "[i]t is important that financial institutions maintain a comprehensive data inventory and a suitable data classification process, and that access to customer data is restricted appropriately through effective identity and access management." The data inventory process extends to data held by vendors.

Use of the cloud may involve unique controls and requirements, including with respect to backup systems (and the location of those systems) and the return and/or deletion of protected data upon contract termination. The FFIEC warns that cloud storage (and especially "multi-tenant cloud deployment") could increase the frequency and complexity of security incidents. At the end of the day, "[i]f financial institutions are not sure that their data are satisfactorily protected and access to their data is appropriately controlled, entering into a third-party relationship with such servicer may be ill advised."

Legal, Regulatory and Reputational Considerations

On this broad topic, the FFIEC highlights that institutions should consider whether data is stored or processed overseas and/or comingled with other customers' data.

Business Continuity Planning

Business continuity for a financial institution may be more challenging when the cloud is concerned. Thus, a financial institution should consider not only the cloud vendor's business continuity plan, but also how the use of the cloud impacts the financial institution's plan.

* * * * *

In sum, financial institutions should look beyond potential benefits of cloud computing and perform a thorough due diligence and risk assessment of elements specific to the service. As with any outsourcing, financial institutions (and others) are expected to assess risks on an ongoing basis and make prudent decisions and adjustments regarding security of their information systems and storage.

Not Addressed in the Guidance

Although not specifically addressed by the FFIEC, it is also important to note that if the institution handles Protected Health Information regulated by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the institution may be a "Business Associate" and subject to HIPAA security requirements. This may occur when the institution provides lock box services, accounts receivable and payment management, and check printing to health care providers or insurers. Certain states, including Texas, are also implementing aggressive laws requiring businesses that handle health information to meet requirements that can be more stringent than HIPAA. Both HIPAA and state law require notification of security breaches. HIPAA compliance is not insurmountable in the cloud, but regulatory requirements can certainly be unique.

For more information on the matters discussed in this Locke Lord QuickStudy, please contact the authors:

Bart Huffman | T: 512-305-4746 | bhuffman@lockelord.com
Tammy Ward Woffenden | T: 512-305-4776 | twoffenden@lockelord.com
Jennifer Rangel | T: 512-305-4745 | jrangel@lockelord.com