Cloud Computing for Financial Institutions

PUBLISHED ON
May 4, 2020

A federal banking agency has taken aim at cloud computing, offering financial institutions guidance and proposed safeguards in the new world of data processing and storage.

The purpose of the Federal Financial Institutions Examination (FFIEC) recently issued a joint statement on cloud computing falls in line with its principal responsibility - to prescribe uniform principles and standards for financial institutions - by addressing the widespread use of cloud computing services by its member financial institutions and presenting an overview of related security risk management principles.

The FFIEC is a formal government interagency body composed of five banking regulators members - Federal Reserve Board of Governors, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency and the Consumer Financial Protection Bureau.

Businesses have been quickly moving some or all of its technology resources, including its software, platforms, and infrastructure, to the cloud because of the considerable expense that cloud computing can offer over "on-premise" equivalents. With concerns over a worldwide economic depression because of the effects of the COVID-19 virus, many financial institutions will likely be seeking cost-cutting measures, and moving to cloud computing could be an easy financial decision.

Cloud computing can also deliver high speed, allow excellent accessibility and also has perceived increased security. However, the FFIEC's statement is issued following several significant security breaches involving cloud computing services (including the breach that affected Capital One last year, which involved cloud computing provider Amazon Web Services). Despite such breaches, the FFIEC anticipates more financial institutions moving to cloud-based resources. The statement emphasizes the importance of an institution's ever-present "sound security controls," which includes its understanding of the shared responsibilities between it and its cloud service providers. The FFIEC also uses its statement as a cautionary reminder that financial institutions should not assume effective security and resilience controls exist simply because its technology systems are operating in a cloud-computing environment.

The statement provides overviews of risk management practices for financial institutions to follow toward safe and sound use of cloud computing services. It also includes additional safeguards to protect customers' sensitive information from risks that pose potential consumer harm. These practices include examples relating to a financial institution's IT governance, cloud security management, change management, resiliency and recovery, audit and controls assessments. For instance, in the area of cloud security management, the statement provides that management of a financial institution should consider each of the following questions when evaluating its cloud service provider and resources:

• Do the cloud service provider's security controls support the financial institution's systems and information assets that reside in the cloud environment?

• What types of oversight and monitoring activities should the financial institution require of the cloud service provider, including the types of compliance reports and independent assurance reviews, such as audits, penetration tests, and vulnerability assessments?

• Are there additional personnel controls, such as background checks and security awareness training, necessary for the service provider's staff that supports the financial institution's operations or has access to financial institution data?

The statement also provides a helpful list of government and industry resources and references to assist financial institutions using cloud computing services. The statement notes that there are also many industry-recognized standards and resources that can assist financial institutions with managing cloud computing services, such as National Institute of Standards and Technology, the Center for Internet Security's Critical Security Controls and the Cloud Security Alliance.

If you have any questions on this new guidance or how you are required to protect your data in the cloud, please contact me or any member of the Barley Snyder Finance & Creditors' Rights Practice Group.

WRITTEN BY:

Donald R. Geiter, J.D., M.S.L. (Cybersecurity Law & Policy), CIPP/US, CIPM

Partner

Tel: (717) 399-4154

Email: dgeiter@barley.com