THE
NATIONAL LAW REVIEW

The Newest SEC OCIE Risk Alert: Cloud Storage Is Great, If Your Cloud Is Secure!

Friday, June 14, 2019

Article By Greenberg Traurig, LLPAlerts
Paul Ferrillo

Communications, Media & Internet
Securities & SEC
Consumer Protection
All Federal

Nearly every day we learn of another company leaving tens or hundreds of millions of pieces of data or personally identifiable information on an unsecured database for anyone to see (or steal). It is no wonder, then, that the SEC's office of Compliance Inspections and Examinations (OCIE) has issued a Risk Alert on the importance of storing customer and data in a cloud environment in a secure fashion.

The Risk Alert, titled "Safeguarding Customer Records and Information in Network Storage – Use of Third Party Security Features," identifies a number of concerns. One problem not specifically discussed, however, is that aside from technical and other errors, some registrants operate under the erroneous perception that as between the registrant using cloud storage for its data, and the cloud service provider itself, it is the *service provider* that is "responsible" if data is lost or stolen. While agreements and industry practices may create obligations that run from the provider to the registrant, the SEC will first look to the *registrant* for failures to protect customer data.

As between the registrant and its service provider, there is a "shared" responsibility for cloud data security more completely defined by their service level agreement (SLA). As a rule, "[u]nder the Shared Responsibility Model, the CSP [cloud service provider] is responsible for 'security ***of*** the cloud' which includes the hardware, software, networking, and facilities that run the cloud services [better described as the "infrastructure" of the cloud]. Organizations, on the other hand, are responsible for 'security ***in*** the cloud' which includes how they configure, secure their data [e.g., through encryption] and use the resources provided by the CSP." *See* "A Comprehensive Guide To Preventing Cloud Misconfiguration" (The Cloud Guide).

This is all good, assuming the firm understands how to set up storage in the cloud, and what "buttons need to be clicked" to make their data as fully secure as possible. Sometimes that is entirely possible, if the IT skill level is there. But despite the best efforts of the firm, errors can be made. One recent report noted that "cloud misconfiguration remains the biggest security threat for organizations in the cloud, but it is also preventable. The reason is that human error is the most common cause of misconfiguration. The 2018 IBM X-Force Report notes a 424% increase in data breaches resulting from cloud misconfiguration caused by human error. Gartner indicated that by 2020, 95% of cloud security incidents will be the customer's fault." *See* The Cloud Guide.

Given the statistics on cloud breaches, it is no surprise that OCIE issued the Risk Alert on proper cloud storage practices, and in particular, what potential problems the registered investment adviser and broker-dealer community should be on guard to avoid or control. OCIE hinted at some of the problems in its opening paragraph: "Although the majority of these network storage solutions offered encryption, password protection, and other security features designed to prevent unauthorized access, examiners observed that firms did not always use the available security features. Weak or misconfigured security settings on a network storage device could result in unauthorized access to information stored on the device." (Emphasis added.)

Based upon its observations in other registrant examinations, OCIE also noted in the Risk Alert some potentially problematic issues pertaining to cloud storage solutions:

Misconfigured network storage solutions. In some cases, firms did not adequately configure the security settings on their network storage solution to protect against unauthorized access. In addition, some firms did not have

policies and procedures addressing the security configuration of their network storage solution. Often, misconfigured settings resulted from a lack of effective oversight when the storage solution was initially implemented.

Inadequate oversight of vendor-provided network storage solutions. In some cases, firms did not ensure, through policies, procedures, contractual provisions, or otherwise, that the security settings on vendor-provided network storage solutions were configured in accordance with the firm's standards.

Insufficient data classification policies and procedures. In some cases, firms' policies and procedures did not identify the different types of data stored electronically by the firm and the appropriate controls for each type of data.

OCIE concluded its Risk Alert by noting, based on its examinations, several strategies that worked regarding effective configuration management programs, data classification procedures, and vendor management programs, including the company having:

Policies and procedures designed to support the initial installation, on-going maintenance, and regular review of the network storage solution so that it meets on-going security requirements;

Guidelines for security controls and baseline security configuration standards to ensure that each network solution is configured properly from initial use and thereafter; and Vendor management policies and procedures that include, among other things, regular implementation of software patches and hardware updates followed by reviews to ensure that those patches and updates did not unintentionally change, weaken, or otherwise modify the security configuration.

We add to OCIE's list several more specific strategies regarding the security of cloud storage that should be considered by registrants:

- Continuous vulnerability assessments regarding the cloud storage platform itself for potential problems and updates, especially if the firm's architecture or storage needs grow over time;
- Strong Identity and Access Management Solutions so that only those who should be accessing the data can actually access it, though in a secure fashion – with access categorized so that even authorized users can access only those parts of the data set that are required for their duties;
- A strong password policy with mandatory multi-factor authentication;
- For some storage or cloud services, access to the data sets can be completely blocked from public access by a flip of the switch (like Amazon's Block Public Access feature). This is a very good idea to keep data out of the hands of those who should definitely not have access; and
- Encryption at rest and encryption in motion should be strongly be considered to protect any data stored in the cloud.

For many, the cloud has been a godsend both for storage, convenience, and IT costs savings. But the past year has shown that in the rush to savings, people sometimes forget about security issues. Rest assured, the SEC has not forgotten about them. OCIE's May 2019 Risk Alert provides not only proof of this, but important strategies for keeping customer data safe in the cloud.

Source URL: https://www.natlawreview.com/article/newest-sec-ocie-risk-alert-cloud-storage-great-if-your-cloud-secure