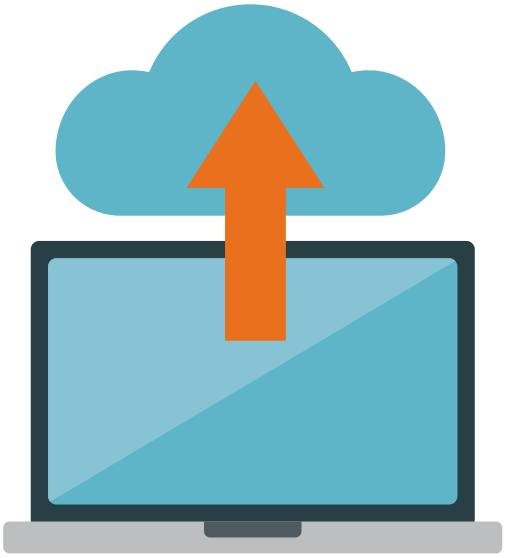
#ForensicPerspectives

6 things to review with your cloud service providers



When corporate data are moved to the cloud, key access logs and other forensic artifacts can get moved as well. Follow the tips below before an incident occurs to ensure that your incident response team can preserve access to these critical data stores.

Activate access logs and tracking

Ask your cloud provider to activate access logs and other tracking mechanisms. Confirm that the logs are being retained for the time period that matters to you.

Negotiate a response agreement

Memorialize a service level agreement with your cloud provider that includes breach incident response. This should include a process, a price, and an agreed-upon response time.

Hold "fire drills"

Periodically test access to audit logs and ensure that your cloud service provider can provide the necessary details.

Validate scalability

You may have a plan in place to search a single mailbox or a single day's worth of activity. However, can you quickly and effectively search for evidence of intrusion across all employees over a multiple-month time frame?

Confirm everything

Does your cloud provider have the desired security? Insurance coverage? Cyber disaster recovery protocols in place? Confirm all of these things periodically.

Find an independent expert

Retain an experienced incident response team via outside counsel to reasonably establish and preserve attorney-client privilege. This is vital since it is likely that the findings and conclusions will be of significant interest to third parties who will have interests adverse to your own.

Kristofer Swanson, CPA/CFF, CFE, CAMS | Vice President & Practice Leader, Forensic Services
+1-312-619-3313 | kswanson@crai.com