# Cloud Third-Party Risk Assessment

James Baker, CISSP-ISSAP CISM

# Ultimately, why do we perform Cloud Third-Party Risk Assessments?

We can’t outsource liability!

A number of resources make this claim but couldn't determine the originator, and this was before cloud.

- 71% of companies fail to adequately manage risk of third-parties!

Herein lies the problem!

- Define adequately and legally who makes the determination if you have adequately managed the risk of putting data in a cloud?

Because “adequately” is so subjective and possibly costly, it can lead to the demand for too much transparency.

# Most important part of cloud third-party risk management?

## what's a MSA

**Master Services Agreement**

**Sit eu patrioque**
Usu option detracto ut, ius ullum mundi gloriatur ne. Dolorum deleniti singulis in vim, case dolorem erroribus ne sit, vix paulo latine id. Eos honestatis cotidieque in, pro odio ludus tacimates ne. Mutat mediocrem reprehendunt ne est, ne autem luptatum duo.

**Vidisse gloriatur**
Quo quem sanctus argumentum in, scripta civibus democritum at mel, ea eos solum doming liberavisse. Ea nisl modo ius. Eam ea habeo feugiat suavitate, id agam suscipiantur cum. Vidisse gloriatur at sit. Id probo nihil postulant sea.

**Mucius disputationi**
Adhuc ancillae delicata vis ad. Mea omnes affert similique ea. Cu vim alia voluptaria. Id alia mnesarchum vim, ei est illud option verterem. Mucius disputationi ne mea, aperiam scripserit te pri. Sit eu patrioque assentior.

**Mel libris**
Mediocrem erroribus eu eum, ius unum veniam iuvaret ei. Ad pro odio reprimique, omittantur ullamcorper est ei. Veniam oportere suscipiantur vix no, ei duo libris detraxit. Mel libris noluisse quaestio cu, est eius ignota instructior an. Te sit docendi indoctum intellegebat. Decore docendi complectitur at mei, ius oblique volutpat ex, dicam officiis splendide pro ea.

**Habeo repudiare**
An vel deleniti efficiendi, eu vim natum labores, qui ei hendrerit gloriatur democritum. Cu mea habeo voluptatibus. Iriure inermis in duo, duo adhuc latine antiopam eu. Aeque graeco dolorem ei mel, in quaeque appetere moderatius cum. Habeo repudiare no nec.

contract

details services to be provided

will be dense

# Why?

- Provides the right to audit
- Defines information security, data protection or privacy requirements that the cloud provider must have in place in order to do business together
- Gives the customer the ability to end the contract without penalty if the cloud provider can’t meet information security, data protection or privacy requirements

# Ideas on what you should require from your cloud provider in an MSA? (In contract language)

- The right to perform an in person audit based on the given security requirements
- For SAAS offerings, require an annual web application pen test performed by a reputable third-party vendor using industry standard methodology and provide an Executive summary of the results
- The cloud provider have a formal risk management process in place that provides detail on when vulnerabilities will be mitigated based on their severity
- Mandate that the cloud provider have a dedicated security professional or team in place with a certain number of years experience and or certifications.
- Require a third-party assessment or audit i.e. SOC 1/2 type 2
- All communication of data over untrusted networks will be transmitted using industry standard encryption.
- One DR test per year and show proof, formal Incident response program or eDiscovery program etc.....

# What info shouldn't be required from a cloud provider in an MSA or a questionnaire?


- Any document that provides info about vulnerabilities that are specific to a URL or IP address
- Any policy or procedure that provides command line info or info about security technology's in use (View over
- Detailed architecture diagrams WebEx or in person)
- The right for one of your people to perform web application or network layer penetration testing
- Excessive testing i.e. more than one DR test per year

# Why Not?  Too much transparency

# Developing a questionnaire



Final
Thoughts

# Contact Information

jbaker@clouddefenders.com


@ABCecurity