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 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 WebEx or in person)
• Detailed architecture diagrams
• 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@clouddfenders.com

@ABCecurity