In the Cloud

Risk Assessments in the Great Unknown

Agenda

- Re-Define “Cloud”…again
- Define the Risk Assessment Process
- Table Stakes
- Table Stakes Backed in Writing
- The norm vs. The cutting edge
- Success!
- Questions

Re-Defining the “Cloud”…again

- **What is a cloud?**
  - a visible mass of condensed water vapor floating in the atmosphere, typically high above the ground.
  - a state or cause of gloom, suspicion, trouble, or worry.

- **Cloud defined for business**
  - Not on premises (simple, inelegant, but it works)

- **Hybrid cloud**
  - Some on premises and some not on premise but the off premises is required for functionality.

- **Why re-define?**
  - Needs to be easy to understand, easy to risk assess and easy to define contractual obligations.
  - If your clients or business units can‘t easly describe and understand a cloud envinroment, how do you expect them to be aware of the protection required?

Risk Assessment – The Process

- **The good news!**
  - Your current methodology for assessing risk and performing audits will work!
  - You still have to ask all the same questions
  - You still have to have the stakeholders involved
- **The bad news!**
  - You will be limited to what you have access to (even less if you don't' have a solid contract to work from).
  - Timeliness of information may be limited also by SLAs and contract terms
- **Where to begin?**
  - It begins when the client or company makes the commitment to allow information to be housed outside of it's data centers.
  - Even if you aren't in the loop, where do you start?
  - Eventually those services are going to require a PO and a contract.
  - Procurement is your best friend

Considerations in contract language

- **In order to facilitate the risk assessment discussion, Procurement is your first line of accurate information.**

- **Contract considerations from internal clients include:**
  - **Will PII or PCI data be exchanged?**
  - **Will information be stored and for how long?**
  - **Where and How will information be stored?**
  - **Who will have access to information?**
  - **Use of Contractors**
  - **Use of Third Party Facilities**

Table Stakes

What are the table stakes for cloud providers?

- **Secure Data Transport**
- **Encryption in storage**
- **Strong user authentication mechanisms**
- **Multi-factor authentication for administration**
- **Data Classification scheme**
  - **understood**
  - **defined**
  - **enforceable**

Table Stakes – Backed in writing

What are the table stakes for cloud provider contracts?

- **Location of Data Storage (US, Global)**
- **Background Checks on the Service Provider and their Consultants**
- **Appropriate Reps and Warranties**
  - **The Service Provider knows the purpose of the engagement from the Customer point of view**
  - **The Service Provider has experienced people trained to perform the specific task**
  - **The Documentation adequately describes the Service**
  - **The data will be managed securely**
  - **Service Provider will be responsible for their subcontractors**

Table Stakes – Backed in writing

- Cyber and E&O Insurance
- Proper and Timely Notification of Data Breach
- Indemnification for Claims
- Injunctive Relief and Termination Rights
- Audit Rights

The norm vs. the cutting edge

- Some providers have extended their capabilities beyond the minimums.
- When evaluating these services in a risk assessment, the protection should always be commensurate to the value of the data.

- Advanced User Access
  - IP based or Geolocation
  - Time based coupled with Geolocation
  - Dynamic user based authentication base on IP address, Geolocation and Time

- Data usage
  - Dynamic data store access and field level masking and encryption on the fly
  - Understanding what normal looks like, everything else is masked or encrypted until approved.

Success!

- Beyond awarding the contract, what leverage do you have?
- There are several wins in driving negotiations for a cloud vendor from a risk perspective.
- Increased Business Opportunity
- Lower's their Risk
- What is Fair and Equitable

Success?

- You’ve assessed the risk, now what?
- If the assessment is performed prior to going live, during the contract period there is a great opportunity.
- If the assessment is performed on existing cloud services, there will be limitations to what can be achieved.
  - Is there an opportunity for an addendum?
  - Is the contract coming up for renewal soon?
  - Risk acceptance sign off by executives with understanding and quantification of the potential impact.

Questions?

Eric Ballantyne eballant@jcp.com

Tracy Vowell tvowell@jcp.com