Fast & Flexible
Data Privacy Risk Analysis
For Technology Procurement In Higher Education

Presented by
Raymond Hsu, CPM & William Li, Esq., CISSP
rayshu@uw.edu  wml@uw.edu
More enterprises shifting to the cloud...

Cloud Computing Infrastructure And Platform Market
($ billions, 2013-2018e)

Source: Goldman Sachs Research

Global cloud service revenue from storage services from 2010 to 2016 (in billion U.S. dollars)

Source:
Forbes, Gartner
© Statista 2015

Additional Information:
Worldwide, Gartner: 2010 to 2012
The type of corporate data stored in the cloud is also the data most at risk.

As shown in Figure 3, customer information, emails, consumer data, employee records, and payment information are most often stored in the cloud. Since 2014, the storage of customer information has increased significantly from 53 percent of respondents to 62 percent of respondents.

Source: Ponemon Institute, 2016 Global Cloud Data Security Study
Procurement and Security working together

> Enable organizations to leverage cloud
  - Flexibly and efficiently expand enterprise systems
  - Access to an expanse and growing solutions market
  - Make informed decisions about risk
  - Create opportunities to manage risk

> Evaluating I.T. Vendor Offerings Is Key
Challenges

> I.T. Procurement (Generally)
  – Innovation is valuable, but newness can complicate
  – Multiple disciplines of jargon

> Education Procurement (Specifically)
  – Complex institutional missions
  – Conflicting business interests
  – Leads to nuanced approach to “Confidentiality, Integrity, Availability”
  – Scrutiny on a shoestring
UW “DSPA” Solution: A Method of Analysis

> Proforma “Data Security & Privacy Agreement” + Analytic Rubric
  – *Flexible* method of analysis
  – *Not* a worksheet to compute a formula

> Focus: Practical for a procurement timeframe

> Approach:
  – *contracting risk due to the relationship with the vendor*
  – *Not* “how would we have implemented this”

> Public as a philosophy

https://ciso.uw.edu/resources/risk-mgmt/external-data-sharing/
Overall Contracting Philosophy and Goals

> Goals: What you hope you get
> Philosophy: How you hope to get there
> Philosophy + Goals = Strategy

Strategy should be
> Mission driven
> Practical
Practical Considerations in Crafting the DSPA

> Procurement Workflow
> Communicate Vendor Expectations
> Sequence provisions logically
> Form a contract

CONTRACT FORMATION:
- Parties manifested mutual assent
- to a definite bargain
- supported by sufficient consideration to make the promises enforceable

iv. If the Work, in whole or part, involves access or delivery of information via a public-facing web site, then Vendor represents and warrants that its current privacy policy is published online, and is accessible from the same web site as any web-hosted application that is a part of the Work. Vendor’s privacy policy will
The Evaluation Rubric Applies: Whether vendor reads your proforma agreement or not!

EXECUTIVE SUMMARY

The Overall Position is less than acceptable; a renegotiation strategy is recommended.

The University has defined information security and privacy goals for contracting with third parties. The goals which suffer the most significant strain are maintaining Ownership of UW data and security and privacy guarantees. With respect to other scored attributes, the findings are:
- **Flexibility to improve the University’s position relative to the goals may be limited**: limited may be overly rigid because the issues at stake touch the fundamental business model.
- **Although there are temporary gaps about information security and privacy maturity, the vendor appears to be capable of meeting University security and privacy goals**: Low levels of alignment between internal controls and vendor controls may lead to a dissonant situation.
- **Efforts are in the estimated effort needed to remediate these gaps**: Further includes the quality of the transaction, and cooperation of the vendor.
- **Mutually secure fitness of the vendor to perform**: Further includes vendor’s technical aptitude, due care philosophy, and insurance coverage.
- **Overall clarity and the degree to which existing with the vendor will be an additional burden or internal unaligned effort**: Further includes diversity of role responsibilities, related resource alignment, and transparency of contact interfaces.

The platform will initially integrate data feeds from UW’s HRIS and will transition to a full integration. Large volumes of personal and confidential data about students is involved.

COMPOSITION OF THE AGREEMENT

- This analysis examines the following documents:
  - Master Services Agreement (MSA)
  - Business Associate Schedule (BAS).
  - This document takes precedence over the MSA.
  - This is the assignment of all the obligations of the MSA, but with the understanding that UW may also be able to make unilateral changes to its policies.

METHODOLOGY

This analysis is informed by security and privacy risk. Specific observations and recommendations were reviewed, and in this analysis the following documents and supplemental analysis may be available.

OBSERVATIONS AND RECOMMENDATIONS

**TOPICS FOR FURTHER CONTRACT DISCUSSION**

- Should commit to a “know or should have known” standard of care with respect to protecting personal or privacy data.

- Does not appear to have made a contractually binding guarantee that it will exercise an appropriate level of care (“due care”), especially for confidentiality and integrity. It seems to be contractually limiting its duty on this matter.

- Information Security and Privacy Analysis (ISPA)
Using the DSPA

The following flow chart illustrates how to use the DSPA:

Start

- Unsere DSPA Needed?
  - Yes, the solution will be important to organization's mission
  - Yes
    - Send DSPA to Vendor (Include as early as possible)
    - Substantial markups to DSPA?
      - Yes
        - Email cisco@uw.edu
        - Together we will analyze the risk
      - No
        - Execute agreement for transaction
  - No
    - Critical System or Confidential UW Data?
      - Yes
        - Communicate clarifications
      - No
        - Email cisco@uw.edu
        - Together we will review outcomes

Informed risk decision
The ancient ruins at 1 Hacker Way, Menlo Park, CA

> Longevity in technology and academia are measured on different scales
> Tech companies understand their own business survival risk, you should too
“Winning” the negotiation versus Making a good decision

> Consider
  - What else, besides data (and payment) does the vendor need to perform the work?
  - Visibility and leverage are needed to administer the executory contract
  - What circumstances does the agreement need to anticipate?

> Identify stakeholders who really understand
  - What is at stake for the institution
  - What the vendor must deliver
  - What data is needed for the vendor to successfully perform