Evaluating Third Party Services

Michael Corn
Chief Privacy and Security Officer
A Few of my Favorite Things

- Box.net
- Dropbox
- Mozy
- iTunes
- Gmail
FORMS OF ALTERNATIVE SOURCING IN USE

• 49.8% Application Software Via the Internet (SaaS)
• 19.1% 3<sup>rd</sup> Party Provided ERP Project Management
• 18.8% 3<sup>rd</sup> Party Provided Network Design
• 14.2% 3<sup>rd</sup> Party Operated Help Desk (e.g., call center)
• 9.4% 3<sup>rd</sup> Party Managed Network Operations
• 9.1% Internet or Cloud-Based Servers
• 7.8% Internet or Cloud-Based Storage
• 7.4% Primary Data Center Provided By A 3<sup>rd</sup> Party
• 7.1% 3<sup>rd</sup> Party Provided Desktop Computing Support
• 4.5% Internet or Cloud-Based Security Applications
• 3.6% Internet or Cloud-Based S/W Dev Environments

ECAR Alternative IT Sourcing Study, September 2009
Basic Risk: Strategic Dimensions

- Loss of control
  - Inability to control/influence the evolution of a service
  - Inability to define security policy with high level of assurance
- Potential loss of organizational expertise
  - [http://www.educause.edu/Resources/StrategicOutsourcingandCloudCo/173358](http://www.educause.edu/Resources/StrategicOutsourcingandCloudCo/173358)
- Forces a close reexamination of the mission of IT within higher education
BASIC RISK: YOUR Data – NO CONTROL

- What is the meaning of “no control”? No control over:
  - Where it is
  - How it is used
  - With whom it is shared
  - How it is protected
  - How long it is kept
  - Who owns it
  - How available it is

Regardless of how or what you procure, you must ask and answer these questions!
Addressing Risk

- **2006**: focus on contract
  (https://wiki.internet2.edu/confluence/x/kQId)

- **2009/10**: focus on low-risk purchases
  (http://go.illinois.edu/essa)

- **2011**: focus on quantifying vendor evaluation
Vendor Assessments

• Home Grown
• Demonstration of some standard (e.g. SAS 70 II, or SSAE 16)
  – http://www.csoonline.com/article/622277/sas-70-replacement-ssae-16-
• Consortium assessments: Shared Assessments
  – http://sharedassessments.org/
Homegrown Model: Northwestern U.

- Service Provider Security Assessment
  - Each provider completes a questionnaire
  - Quantified summary used by University executives and business unit to evaluate risk

(samples courtesy of Dave Kovarik at NWU)
## B. Site Details

<table>
<thead>
<tr>
<th>Question</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>B-1. Where is the Service Provider’s primary production site located?</td>
<td></td>
</tr>
<tr>
<td>What is the tier rating and applicable standard of this datacenter?</td>
<td></td>
</tr>
<tr>
<td>B-2. If Service Provider has an alternate (backup) site, where is that located?</td>
<td></td>
</tr>
<tr>
<td>What is the tier rating and applicable standard of this datacenter?</td>
<td></td>
</tr>
<tr>
<td>B-3. Would Service Provider accommodate Customer’s request and allow for a site visit for a security audit, given 48 hours notice?</td>
<td></td>
</tr>
<tr>
<td>B-4. Service Provider has and will provide summary results of a third-party external Information Security assessment conducted within the past 2 years (SAS-70 Type II, penetration test, vulnerability assessment, SysTrust, WebTrust, etc.). See Request for Documentation.</td>
<td></td>
</tr>
<tr>
<td>B-5. Does Service Provider use other facilities (e.g., collocation) to process or store Customer's data?</td>
<td></td>
</tr>
<tr>
<td>Please provide details: name, location, description of services.</td>
<td></td>
</tr>
<tr>
<td>What is the tier rating and applicable standard of this location?</td>
<td></td>
</tr>
<tr>
<td>Please provide summary results of a third-party external Information Security assessment conducted within the past two year (SAS-70 Type II, penetration test, vulnerability assessment, etc.) for this location. See Request for Documentation.</td>
<td></td>
</tr>
<tr>
<td>B-6. Does Service Provider permit any non-U.S. facility to access, process or store Customer’s data?</td>
<td></td>
</tr>
</tbody>
</table>

## C. Policies, Standards and Procedures

<table>
<thead>
<tr>
<th>Question</th>
<th>Response</th>
<th>Comments/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C-1. Service Provider has formal written Information Security Policies?</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>C-2. Service Provider will provide copies of the Information Security Policies. Where this is prohibited by Service Provider policy, other evidence (e.g., table of contents) will be substituted. See Request for Documentation.</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>
Service Provider Security Assessment

Example “A”

- NU sends STUDENT data (L/C\(R = \text{value of 3}\)) to service provider for reporting on demographics
- Query C-14: Provider has documented Change Control Process. Response is YES (value of 1)
- Risk = (Value of Data) \(\times\) (Level of Control)
  \(-\text{ Risk} = (3) \times (1) = 3\)
Example “B”

- Service provider captures PUBLIC data (value of 1)
- Query D-5. Service Provider has implemented and maintains IDS/IPS technology. Response is NO (value of 3)
- Risk = (Value of Data) X (Level of Control)
  - Risk = (1) X (3) = 3
## Sections and Total Scores

<table>
<thead>
<tr>
<th>Section</th>
<th>Score 1</th>
<th>Score 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>C. Policies, Standards &amp; Procedures</td>
<td>72 (54)</td>
<td></td>
</tr>
<tr>
<td>D. Architecture</td>
<td></td>
<td>42 (42)</td>
</tr>
<tr>
<td>E. Configuration Controls</td>
<td></td>
<td>57 (39)</td>
</tr>
<tr>
<td>F. Compliance Controls</td>
<td>45 (27)</td>
<td></td>
</tr>
<tr>
<td>G. Access Controls</td>
<td></td>
<td>48 (27)</td>
</tr>
<tr>
<td>H. Monitoring Controls</td>
<td></td>
<td>78 (33)</td>
</tr>
<tr>
<td>I. Physical Security Controls</td>
<td>36 (30)</td>
<td></td>
</tr>
<tr>
<td>J. Contingency Controls</td>
<td></td>
<td>51 (36)</td>
</tr>
<tr>
<td>K. Business Relationship Controls</td>
<td></td>
<td>18 (12)</td>
</tr>
<tr>
<td>Low Risk Indication</td>
<td>300</td>
<td></td>
</tr>
<tr>
<td>High Risk Indication</td>
<td></td>
<td>900</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td>447</td>
</tr>
</tbody>
</table>

(nn) = the value representing the lowest risk indication for this section
Shared Assessments

• Extremely extensive questionnaires
  – Short and long form
• Responses “certified” by third-party audit firm
• Provided by vendor on request
Growing list of Service Providers

ACXIOM
at&t
DELUXE CORP
Drivesavers Data Recovery
Early Warning Services
EISI
First Data
IBM
Assessment Options

Standard Information Gathering Questionnaire Version 6.2 (as of 3/24/2011)
Zipped file: The full SIG and the SIG Management Tool

Outsourcers use the SIG as a default questionnaire to streamline vendor assessments. For vendors, the SIG provides a repeatable response to proprietary questionnaires from clients.

SIG 6.1 Level I Questions Only (as of 2/11/2011)
Zipped file: SIG Level I Questions and Information Tabs and the SIG Management Tool

Use the SIG Level I Questions for new service providers and other appropriate relationships (typically low to moderate risk) as indicated by your risk model.
Open Sample SIG file
Near Term Prognostication

- Shared Assessments + Homegrown

- Evolve low-risk expedited process for medium risk

- Create policy and formalize process