Can't Buy Me Love? Then how about a little Privacy and Security?

Assessing Vendor Data Protections

Disclosure to Vendors Can be a Disaster!

- Stanford Medical Center, 2011
- Confidential patient records ended up online
- The marketing agent for Stanford's billing contractor's shared the data with a job prospect
- Mistakes made by the vendor – but Stanford's reputation takes the hit
- Even though Stanford not at fault, it paid $750,000 to settle the lawsuit

Assessing Vendor Contracts

- IT, security, privacy, risk, legal affairs, and procurement are the supporting cast for functional owners
- The same risks and issues apply whether or not there is a fully executed agreement or a standard procurement process
- Low cost and free services may be harder to negotiate, and can be just as risky. "Free" services aren't free, there is always a cost!

What is Vendor Assessment?

- Key elements:
    1. Know your data
    2. Know how the services will affect the data
- Negotiate appropriate data protections – or find another vendor

Privacy Risks

- Data mining
- Data selling/renting
- Targeted advertising
- Data use for purpose other than providing the UC Service
- Release to government demands/requests

Security Risks

- Security breaches (unauthorized access)
- Availability – risk of the service and/or the data not being accessible when needed
- Integrity – risk of data being changed

Compliance Risks

- FERPA
- PCI
- HIPAA
- FISMA (research)
- More...

Primary Tool to Protect UC: Appendix DS

- Use Appendix DS for data-related contracts: specific terms and conditions for data security and privacy
- Prohibits unauthorized use or disclosure
- Requires safeguarding of data
- Requires return or destruction of data upon termination
- Requires vendor to report breaches, and to bear costs

Appendix DS

- Appendix DS largely protects UC on the back end – after a problem occurs, the liability is shifted to the vendor
- But Appendix DS also serves as an important road map for assessing vendors prior to the execution of a contract
- When do we use Appendix DS? It's not always obvious when contracts relate to data
- Get the latest version from your procurement office

Contract Review

- Consider all elements of an agreement: Master services agreement, Terms and Conditions, Privacy Policy, etc.
- Click-through agreements can be binding on the University, not just fully executed agreements
- Just because another university has agreed to a contract doesn't necessarily mean it's a good one

Risk Assessment

- Data inventory
- Privacy Impact Analysis
- Threat Analysis

Technical Review

- Network Diagram
- Data Flow
- Architecture review
- Security review
- Audit analysis

Implementation

- Acceptable Data Use
- Risk summary
- Security or privacy specific provisions

Regular Review

- You're not done yet...
- Regular review of posted terms
- Regular analysis of intended use of service and data
- Regular review of 3rd party audits

Sunset

- Data transfer and disposal
- Breach resolution

Key Takeaways

- It's not always obvious if a contract relates to data, be on the lookout – don't forget free or low cost services
- Use Appendix DS
- Prioritize the most risky contracts; standardize/streamline processes for others
- Just because "it's good enough for them"...doesn't mean it's necessarily good enough for you

Additional Resources

- ITPS
- Privacy Officials
- OGC (including campus counsel, outside counsel)
- Cloud Computing Workgroup
- Campus specific tools – for example:
  - Berkeley Guide to Contracting (available March 2015)
  - UCB Minimum Security Standards for Electronic Information (MSSEI) Self-Assessment Plan Template https://security.berkeley.edu/node/499
  - UCI Guidance on the Use of Cloud Services http://www.security.uci.edu/cloud.php

Questions?