Cloud Services: Policy and Assessment

The skyrocketing popularity of cloud services among faculty, staff, and students is partly a result of the perception that they are not only feature-rich but also inexpensive or even free. Although the usefulness of cloud computing from a feature perspective is undeniable, leaders at higher education institutions are increasingly concerned about the hidden risks, with attendant costs, that are introduced when users share personal and institutional data with third-party providers. Assessing these risks requires a data classification scheme, a relationship between the information security and procurement units, an assessment methodology, and decision-makers (outside of the IT organization) who can act on the risk picture painted by this assessment.

Data Held by Third Parties
Due to many pressures, both internal and external, colleges and universities are increasingly entrusting institutional and personal data to third parties. Tough financial times have forced institutions to cut costs, and contracting with a cloud service is often cheaper than maintaining systems in-house—or at least it appears that way on the surface. It is not always the central IT organization that chooses this option. Academic departments may feel the crunch even more, and they often have special needs that the central IT organization can’t address. An example is the student health center, where staff may want to make electronic health records available to patients. This is not likely an application that the central IT organization would provide, but several options are available in the cloud.

Institutions may also turn to third parties if service is improved. If the central IT organization can’t provide the redundancy, fault tolerance, and universal availability of a cloud service, the sensible decision is to outsource the service so that the institution can focus on improving other core competencies.

One cost of outsourcing that is not always apparent, however, is the risk the institution takes by placing institutional or personal data in someone else’s hands. Though it’s tempting to think that all the risk is transferred, the institution generally needs to show due diligence in vetting the service provider. Also, reputational risk does not seem to be transferable. It is the institution’s logo, not that of the service provider, that will appear over the news anchor’s shoulder should a data breach occur.

Organizing for Third-Party Management
The security risks of outsourcing may seem to be obvious. Most technologists are aware that these risks exist, but they have very little control over the procurement process where the risks can be assessed and addressed. At many institutions, academic departments and even the central IT organization can enter into agreements with third parties without a security assessment. Also, even if members of the security team make an assessment, they may be (appropriately) reticent to make the risk/benefit decision of whether to proceed. That’s why getting a handle on these risks requires a strategic approach.

Institutional leaders may be asking themselves several questions:

- In what situations will we perform assessments?
- How can we participate in the procurement process to ensure that a security assessment occurs?
- Once we’ve measured the risk of a certain arrangement, who will weigh the risk against the benefits and decide whether to proceed?

Without an institutional data-classification scheme in place, determining when to do an assessment and when not to may be difficult. Still, there may be obvious cases in which a review is essential, such as situations involving Social Security Numbers or payment card data. At a minimum, institutions should enumerate all the data types that are sensitive enough to warrant an assessment, so that judgments won’t have to be made for every case. Another option is to publish a policy or standard stating when assessments are conducted and leaving the decision to procurement or the unit entering into the agreement.

After enumerating which data are sensitive enough to warrant assessments, an institution should involve the central procurement unit. Procurement generally has control over whether a purchase goes through. If procurement is willing to flag any agreements that involve institutional or personal data being held by third parties, security has a foot in the door to evaluate those third parties ahead of time.

There are limits, however, to procurement’s control. Making purchases with payment cards is commonplace in higher education. Often, the procurement unit places restrictions on the use of these cards. Per-transaction limits on the dollar amount are one example, often enforced automatically. Unfortunately, the costliness of a service has no bearing on what data the user will choose to share with the service. Some institutions forbid using payment cards to purchase services, reserving them for goods only. Although this practice might seem to ensure that any agreements with third parties go through the procurement unit, it is difficult to enforce in practice. The logical conclusion...
is that institutions must stay vigilant, through other means, for cloud arrangements that slip through the cracks. Policies that prohibit a department from entering into third-party vendor or cloud arrangements without a review are a good means of building a governance infrastructure around this vigilance.

Once the security team performs the assessment, someone must decide whether the risks of the cloud agreement outweigh the benefits. This decision is generally made by the user representative and involves a group of data stewards or a single administrator.

Criteria for Reviewing Third-Party Products and Services

Thus far, we’ve talked about sharing data as if this were a binary operation (the institution either shares or it doesn’t). But what the service provider does with the data is just as important. The following are some examples of questions that should be asked during the assessment process:

- Does the service provider merely process the data, or does it store the data?
- Is the data stored on campus, in a dedicated or shared data center, or in the cloud?
- Do service providers transmit data to other entities?
- Do service providers encrypt data in transit or at rest?
- Are backups stored off-site by the service provider, and are they encrypted?
- When the data is destroyed, is this done in a way that prevents future recovery by attackers?

Reviewing Risks to Information Security

Typically, when a piece of major software or application is acquired for on-campus use, it is subject to some type of assessment regarding its suitability to task, and this assessment includes whether it meets the institution’s needs with respect to security capabilities. This is sometimes referred to as an application software review or internal risk assessment and is frequently done in the context of a Request for Proposal (RFP). The methodology of this review may or may not be standard.

In the case of a hosted system, or what is today referred to as cloud computing, there should also be a review of the security capabilities of the provider, particularly in the context of the institutional data being handled by the provider. Since the system is not coming on-campus, this review is a bit different, focusing on vendor questionnaires, perhaps some type of on-site inspection, and independent assessments such as a SAS-70 or SSAE-16.

These assessment approaches, however, share a number of weaknesses:

- The development and maintenance of an assessment questionnaire is a burden on each institution procuring IT services in the cloud.
- Answering different questionnaires from different prospective customers is a burden on the service provider.
- On-site inspections typically reveal only physical security issues and skip over a variety of other security concerns.
- Attestations such as SAS-70 reports are simply a confirmation, from an independent entity, that the provider is following a list of security measures it submitted to the independent entity—these measures may not be the security measures that are necessary for and desired by the customer.

Shared Assessments

These difficulties when procuring services in the cloud are faced not only by higher education but by other industries as well. In fact, the financial services sector has developed a standard mechanism, known as Shared Assessments (http://www.sharedassessments.org), for assessing the security of third parties. Shared Assessments is a mature methodology, presently on its sixth iteration. It is suitable for use by industries outside of financial services and is available at no cost. Shared Assessments addresses the basic weaknesses (outlined above) in reviewing third parties. As a common standard, it does not have to be developed and maintained in-house, it can be responded to by vendors only once rather than uniquely for each customer, and it covers the entire spectrum of security concerns, ensuring that the provider is covering these concerns and not simply a self-provided list. Shared Assessments is composed of two pieces: the SIG (Standardized Information Gathering) questionnaire, and the AUP (Agreed Upon Procedures), which is an audit template for reviewing compliance with the security measures suggested by the SIG questionnaire. In many cases, the in-depth Shared Assessments SIG questionnaire is overkill. For those projects, a shorter version exists: the SIG Lite, which boils the overall security assessment down to sixty-eight questions.

The use of Shared Assessments when reviewing a third-party vendor ensures that an institution is using a tested approach validated by the financial services industry and its regulators.

Conclusion

Ultimately, cloud services are a variation of third-party vendor data-processing services that have existed for years, and thus there are established models for their governance. An institution should have some sort of policy statement and training material covering the types of information allowed on these services, both without an institutional review and with one. A process should be established for conducting institutional security reviews when appropriate according to the policy. An excellent starting point for such a security review is to adopt or adapt the Shared Assessments tools already in use in the commercial world. With such a policy and assessment process in place, the risks of the cloud can be appropriately assessed and, if need be, either mitigated or even declined.

David Escalante is Director of Computer Policy & Security at Boston College. Andrew J. Korty (ajk@iu.edu) is Deputy Information Security Officer at Indiana University.

© 2011 David Escalante and Andrew J. Korty