The sourcing of IT systems and services takes many shapes in higher education. Campus central IT organizations are increasingly responsible for the administration of enterprise systems and for the consolidation of operations into a single data center. Specialized academic and administrative systems may be run by local IT departments. In addition, the trend toward alternative IT sourcing strategies has turned attention to “above-campus services,” which include services shared among institutions, hosted systems administered by third parties, and cloud computing service arrangements in which the systems and data are distributed among an interconnected infrastructure known as the cloud. Whatever sourcing strategy an organization pursues and wherever the data resides, a set of common challenges and opportunities remains. In this interview, Rodney Petersen explores these issues with three higher education privacy, security, and risk professionals.
had a meeting with a unit that has been running on a single machine behind a single firewall in our data center because they have a lot of sensitive data. But that equipment is end of life, and we’re moving them to a virtual environment, which means that we can respond to equipment failures much more quickly. We can scale almost instantly to anything the unit needs. Overall, these IT sourcing strategies allow us to be more agile and more responsive and to free up resources from those commodity services that we’re considering outsourcing to cloud providers, so that we can focus on what’s important for the campus, which is the academic and research mission.

Also, the fact that cloud computing is such a popular conversation point and is so dominant in the media has allowed me to have conversations with campus executives about the meaning of risk in information technology, and about risks to data, more easily. I used to have to work a little harder to have those conversations. Now campus leaders are asking me these questions, enabling me to do my job.

Cathy Hubbs: Another aspect is that sourcing strategies allow an institution to leverage staff expertise that it might not have the budget to hire internally. In other words, if you’re outsourcing in a particular area, the cloud company, presumably, is hiring leading-edge staff, keeping them well trained and able to handle your needs. In universities, because our staffing budgets are often low, we may not be able to have a deep bench of specialized talent for all services we provide. We may have one or two staff on one particular service such as e-mail, and often those two staff may have additional duties supporting other services at the university. The cloud provider likely will have more staff, with more depth of expertise.

Brian T. Nichols: In addition, moving IT systems and services out to the cloud can give you more space in your data center—space that would normally be taken up by boxes of hardware. So you may be able to gain back some space. And you may be able to redeploy staff to other areas. For example, if you have people focused on e-mail, maybe you can have them working on developing applications down the line rather than handling strictly e-mail.

Petersen: When we move beyond the opportunities and possibilities, what are some of the challenges or risks of the alternative IT sourcing strategies, and how do you frame those for decision makers?

Nichols: The one that bothers me the most is the question of where the data is going to reside. Is it going to be in the United States? Or is it going to be in another country, which is subject to different laws and regulations? Faculty too don’t always understand where their information is being stored. For example, a couple years ago at our institution, a faculty member put some information in an e-mail, and later a request was made for records, including e-mail. The faculty member was surprised that the e-mail was going to be available and could be published in the newspaper. Getting this message out to all the individuals on campus, laying out the risks, is hard to do and is a major area on which we all need to focus.

Corn: The biggest challenge we face is allowing faculty the freedom to use these services as their pedagogical and research needs require. For many faculty, there’s often not a lot of deliberate thought about risk. It’s: “Hey, here’s a shiny bauble, let’s play with it!”

The risk goes back to the more general question of how we deal with cloud providers. We end up spending a ridiculous amount of time negotiating contracts. I can’t tell you what a high percentage of my time is spent on that, and I know this is true at many institutions. I think this
is because we don't have either a legal or a conceptual framework for what I would call a transitive security policy. I can spend as many years as I need polishing and buffing our security and data-handling policy, and then it's all thrown out the window, in effect, when I go into a contract because I'm negotiating with what a vendor will do. Often by the time a contract comes to me for review, somebody—an important functional unit or VIP on campus—has already decided: "This is what we're buying."

There's not a model where I can say to the vendor: “Here is our security policy. Implement it.” I end up looking through each agreement to negotiate specific data elements, document aspects, and add standard language that addresses best practices that were identified twenty years ago as best practices. There's just no elegant way to go through that process. I think that's why we see so many institutions trying to build consortiums around these agreements. But even that route is fraught with work. Many of the vendors we're dealing with are small and rather fragile; they only appear robust because they're relying on the Amazons and other big cloud providers. This is a real problem for us, and I don't see a good solution on the horizon.

Hubbs: I agree with Brian about the data-location challenge and the problem with varying local, state, and national laws.

Another consideration is the inclusion of language around incident response and notification responsibilities. For example, if your university data is stored on the same virtual servers as government and corporate data, and there's a breach, you will need to be sure that your contract states that the vendor will notify you to discuss the appropriate notification actions. This is a potential tangled web that can be untangled if campus risk officers, legal officers, and information security officers are at the table to talk through the risks and ensure that appropriate language is included in the contract.

I also really like Mike's point about a transitive security policy. On our campuses, we security professionals need to have this conversation with our executives about risk appetite in general. That may be a difficult conversation, but it's a topic that needs to be addressed. Most future decisions about risk can be made more easily once overall risk appetite is defined.

**Corn:** In our standard contract negotiations, we always request that if a vendor discovers a data breach, we'll be notified within twenty-four hours. But when we were negotiating one major agreement, the vendor said "Nope." Then we said: "Well, how about forty-eight hours?" They said: "Guess you don't want our product." And we said: "Will you at least tell us about a breach?" They said: "Guess you don't want our product." We had no leverage in that negotiation at all, because we did want it. The vendor simply refused to agree to what I think is a pretty basic request. I wish we could point to some regulation and say: "You have to agree to it."

The other point is about appetite for risk. A while back, after about three years of discussions, our business and financial services group agreed to allow people to use their P-Cards to license low-risk services without going through a contract negotiation. But it was a long process of explaining where there was and wasn't risk. Let's go ahead and move more quickly.

**Petersen:** What are your views about whether or not a remote-hosting service or cloud computing provider could be more secure than a similar service administered by the campus IT organization?

**Nichols:** At LSU, we have an IT Security & Policy Office, consisting of approximately nine individuals who look at data and check for security. I would assume that a major third-party vendor would have a larger group that may be able to do a better job than, say, a one-person university shop. Then again, a third-party vendor that perhaps hasn't been in the business very long may actually be worse than the groups in a lot of universities. I think it is a matter of how long the vendor has been in business, the quality of its staff, how well-known it is in the market, and the extent of its knowledge. Research and investigation are needed before making any decision pertaining to outsourcing a particular system or service.

**Corn:** This is the issue that pushed me into a different camp. I spent years arguing that these cloud services were putting us at risk and that people were just throwing our data into them. Yet, though there are plenty of providers that do a poor job—and this goes to cloud and any sort of outsourcing—the big players have the resources to do it right. We have a really good data center and a really good data center staff, and we have all sorts
of security controls in place, but they pale in comparison to what these big providers can do. Because where we may have a dozen people, they may have five hundred.

Hubbs: Certainly the larger providers can be more secure. The bottom line is a matter of resources that are dedicated to both privacy and security. Our responsibility, as CISOs, is to vet and validate their security controls.

Petersen: What are the strategies, techniques, and practices that a campus can use to be confident that a service provider’s security and other practices are acceptable?

Corn: The critical thing is, first, to make sure the security people are at the table. You want to make sure that you and your legal department have agreed on the language to be used in these types of contracts. You want to understand the negotiation points. You want all of that to be embedded in the procurement process, to the degree possible. In many cases, the contract is just the RFP (Request For Proposals) that the vendor has agreed to. So we put a lot of attention into getting the right language into the RFP to start with.

Hubbs: About a year ago, I introduced the Shared Assessments Program to American University. I talked with our central IT project office about weaving the Shared Assessment questionnaire into our systems development life-cycle process for services that would be outsourced. The assessment tool gave us a consistent, repeatable set of questions to ask when we’re interviewing the finalist vendors. The security team reviews the answers and writes up an executive summary of concerns and recommendations. The selected vendor has its completed Shared Assessment questionnaire added to the contract as an appendix.

We’ve done this successfully in about five instances so far, and we plan on continuing this as a routine process. We’ve added two questions that ask about continuous monitoring and web application vulnerability assessment. The process results in some very interesting dialogue with the vendors and also opens up the minds of the nonIT people, as well as a lot of our business analysts, to hear the types of questions that we’re asking. Shared Assessments is a holistic approach to people, processes,
technologies, and the policies that these companies are using.

Corn: We’re also looking at Shared Assessments very closely. But there are hundreds of these services in use across campus. If we go down the Shared Assessments/contract-negotiation path for everything, we may as well close the institution, because it’s such a slow process. It’s appropriate for large systems or systems involving sensitive data, where there is a lot of risk, but we need to determine the risk involved with these various services and bring the appropriate process to bear. We need to find lightweight ways of allowing access, particularly faculty and researchers, access to these services without going through the bureaucracy surrounding risk assessment. And I say that as the security guy who does all these risk assessments. I would need a staff of six to keep up with the requests for access to these services if I had to go through that heavy workload for all of them.

Petersen: Are there any frameworks or precedents in the risk management profession for approaching risk—in terms of categorizing, classifying, and deciding what level of intensity or resources you’re going to invest?

Nichols: When I was the chief information security and policy officer at LSU, we came up with a high-level, moderate, and low-level risk classification for data. In agreements with third-party vendors, you would also want to include contract language stating that you own the data. The vendor does not own the data. Also important: you may want to incorporate language into the contract stating that if you are going to outsource e-mail, audits/security reviews are conducted on an annual basis to provide assurances that the vendor is following best practices regarding IT security. Do not let the vendor do the audit/security review; ask the vendor to use a third party in order to provide an independent, objective assessment.

Hubbs: We’re still in the process of maturing and perfecting our process. At this point, we have kind of an ad hoc approach. Basically, I tried to put my foot in the door to work with our project office, since pretty much all projects go through that group one way or another. Smaller and midsize projects don’t always have a project manager assigned, but overall, the central IT department has established itself as the resource that can assist people as they move down the path of purchasing or of putting into place IT services, and more often than not, security is brought to the table.

The security team has developed a list of questions that we ask to try to find out whether we should be more—or less—involved. And then we write up risk assessments around the four areas of confidentiality, integrity, availability, and nonrepudiation. We also often supply openended questions for customers to ask themselves—issues that we think are of some concern. We hand those to the customers to think about and make decisions. Basically, we perform a risk profile and say: “Here’s what we see based on what we know.” At the end, we always make sure there is something in writing.

Petersen: Is there any difference in approach or tools that you would use for assessing an external provider versus a campus-based solution?

Nichols: I would want an external provider to supply certain information. How long has the provider been in the market? How big is its staff? What are the qualifications of the staff? For example, are the staff members certified? What data is going to be out there?

Corn: Another aspect of on-campus assessment concerns IT support. Over the last seven or eight years, I’ve noticed a trend line of increasing professionalization of IT staff on campus. Yet when I’m talking to units, especially smaller units that may not be under a college, I find that they often don’t have adequate IT support or professional IT support. So when I’m in these risk assessments, I put a lot of effort into determining the level of support a unit has—the professionalization around their IT management—because I find this correlates very strongly to the likelihood of whether or not they’re going to have a data breach.

Petersen: How do concerns about privacy factor into your outsourcing strategies?

Hubbs: When we moved our students to Gmail a couple years ago, we had a few vocal faculty members who were concerned about student data and student privacy. Their concerns were primarily about whether Google would be looking at and/or selling the students’ e-mails. We listened, and we engaged the faculty in several conversations, building a large FAQ based on those sessions. Using appropriate contract language, we managed to allay their fears. Our experience has been that it is best to provide a forum for people to voice their concerns and then to take those concerns one at a time in order to mitigate any potential risks.

Nichols: Yes, the main thing is to get out there, explain to folks why you are doing this and what the risks are, and address their concerns.

Corn: As I mentioned before, there isn’t a great legal framework within which to negotiate. A lot of what we’re arguing for is privacy protections for our students, our faculty, our staff, and our data. Again, I wish we had a little more impetus from
the regulatory standpoint to make those negotiations a little easier for us.

Petersen: What can higher education associations do to assist campuses in addressing the privacy, security, and other policy challenges associated with alternative IT sourcing?

Hubbs: It would be helpful if associations could leverage the collective higher education power to provide stronger contract negotiation power around privacy and security issues.

Nichols: I think it would be very, very helpful to everyone in higher education for these organizations to continue to provide resources, on the Internet and in forums and meetings, so that our business officers and all the other users in higher education can have access to information in these different areas.

Hubbs: Perhaps all these great resources could be quantified. For example, “Out of 2,100 members, 1,500 use Shared Assessment.” Or institutions could add TripAdvisor-like ratings, with universities writing up their experiences with certain resources and grading the usefulness of those resources. Another idea might be for several organizations to come together and create a sort of “Good Housekeeping Seal of Approval” to validate the security of technology services.

Corn: I agree. I think organizations can help by giving a stamp of certification to certain services and processes and can be an effective advocate for us with vendors and service providers. By signing up with a Shared Assessments type of service or providing audited information, an institution would receive a public pat on the back to say “Good job.”

© 2011 Michael A. Corn, Cathy Hubbs, Brian T. Nichols, and Rodney Petersen. The text of this article is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 3.0 License (http://creativecommons.org/licenses/by-nc-nd/3.0/).

Rodney Petersen (rpetersen@eduroam.org) is Senior Government Relations Officer and Managing Director of the EDUCAUSE Washington Office. He is also the EDUCAUSE staff liaison to the Higher Education Information Security Council.