This Issue: Network Management and Security
Tired of Unexpected Turns?

CallXpress is today's future proof choice, no matter where the road leads you.

Let's face it. In these times, choosing the right road to build your communications infrastructure can be extremely challenging. CallXpress from AVST straightens the road by enabling you to implement Unified Communications capabilities today while protecting and extending the useful life of your existing data and telephony infrastructure investments – now and into the future.

For nearly three decades, AVST offers organizations ever-increasing new technology. CallXpress delivers advanced call processing, voicemail, unified messaging, personal assistant, fax, speech and notification capabilities – turning your telephone system into a productivity tool.

Enable your organization to work smarter today. Discover how the Investment Protection Program can help future proof your investments.

**STIMULUS PACKAGE PRICING**

Don’t Delay! Every CallXpress system is now discounted for a limited time. CallXpress includes advanced call processing and voicemail functionality, plus 50 unified messaging and personal assistant user licenses.

**MINIMIZE USER RE-TRAINING WITH A FREE ALTERNATE TUI**

Select from a variety of alternate Telephone User Interfaces (TUI) that mimic the Nortel Meridian Mail, Octel®, Avaya® INTUITY™ AUDIX® and other popular first generation voicemail systems — a $3,520 value.

**FREE ON-LINE ADMINISTRATOR TRAINING COURSE**

Administrators can quickly learn to configure and maintain their CallXpress systems in this self-paced web training course — a $600 value.

**PLUS OUR FUTURE PROOFING GUARANTEE**

We understand the PBX you have today might not be the one you have tomorrow. Our Future Proofing Guarantee provides a free PBX software integration when you are ready to transition to IP or planning a change to your existing switch.

Act now. Limited time future proof incentives.

To learn more, visit: [www.avst.com/future-proof](http://www.avst.com/future-proof)
<table>
<thead>
<tr>
<th>Event</th>
<th>Date</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summer Seminar</td>
<td>July 18–21, 2010</td>
<td>The Palace Hotel</td>
</tr>
<tr>
<td></td>
<td></td>
<td>San Francisco, California</td>
</tr>
<tr>
<td>Fall Seminar</td>
<td>October 24–27, 2010</td>
<td>Sheraton Premiere at Tyson's Corner Metro DC</td>
</tr>
<tr>
<td>Winter Seminar</td>
<td>January 9–12, 2011</td>
<td>Pointe Hilton at Tapatio Cliffs Phoenix, Arizona</td>
</tr>
<tr>
<td>Annual Conference</td>
<td>April 3–6, 2011</td>
<td>Hilton Bonnet Creek</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Orlando, Florida</td>
</tr>
</tbody>
</table>

ACUTA's Core Purpose is to support higher education information communications technology professionals in contributing to the achievement of the strategic mission of their institutions.

ACUTA's Core Values are:
- Encouraging and facilitating networking and the sharing of resources
- Exhibiting respect for the expression of individual opinions and solutions
- Fulfilling a commitment to professional development and growth
- Advocating the strategic value of information communications technologies in higher education
- Encouraging volunteerism and individual contribution of members
FEATURES

10
Ahead in the Clouds: Is Outsourcing Right for Higher Education Technology Services?
Geoffrey Tritsch
Tritsch examines the issues a campus should consider when determining how outsourcing best fits into the institution’s technology management strategy.

15
Security: Prepare to Lose Some
Curt Harler
With specific examples and words of advice from Temple University as well as several technology industry leaders, Harler explores some of the security vulnerabilities and best practices campuses should consider.

20
ADVERTORIAL: Which Way Is Up?
The Center for Technology Leadership
Learn more about the program offered by the Center for Technology Leadership as you climb the ladder to CIO.

24
Mobile Security in the Middle
Elwin J. McKellar
Wentworth Institute of Technology and Washington University in St. Louis provided answers to four pointed questions about security issues at these two diverse institutions.

28
Things You Might (or Might Not) Know about Convergence Planning
Mike Grunder and Paul Kirvan
If it’s time for your campus to consider convergence, here are some steps you will want to take to ensure that you do it right.

32
Reviewing the Lessons from Security 101
Janet Hutton
At the most basic level, the campus phone system is both a resource and a portal. This article is a reminder of its vulnerability and the need for security.

34
How Universities Can Persevere in the Security Marathon
Dan Durbin
Juggling to keep a university system open and accessible while maintaining a secure network takes discipline. Durbin offers some good advice for outdistancing would-be spoilers.

37
Security Snapshots of Three Campuses
Miami University of Ohio, Notre Dame, and Texas A&M University provide a snapshot of the approach to security on their campuses.

COLUMNS

6
President’s Message
Matthew K. Arthur
Washington University in St. Louis

8
From the Executive Director
Jeri A. Semer, CAE

40
Q&A from the CIO
Joanne Kossuth
Franklin Olin College of Engineering

ADVERTISERS’ INDEX

38
Thanks to the companies that support ACUTA by advertising in our Journal.
Touchscreen Meets Desktop.
The German quality IP phone snom 870 with touchscreen is available in black and in white. Whatever looks the best on your desktop. Make the choice!

GSA snom IP phones now GSA certified

Special pricing for ACUTA members!
Contact us at infoUSA@snom.com
Tennis matches go five sets. Football games last 60 minutes. The security game never ends.
Ciena's acquisition of Nortel® Metro Ethernet Networks (MEN) accelerates the pace of next-generation networking innovation, giving you the power to deliver what's next. Now.

Visit Ciena.com to learn how our solutions help your institution build the capacity and flexibility demanded by cloud computing applications.

* "Nortel" is a trademark of Nortel Networks, used under license by Ciena.
Anytime you start thinking about security, whether in relationship to networks (wired or wireless), data, laptops, or your house, I suggest that taking a step back to get a wider angle on the picture in question is a wise thing to do. Too often security is a knee-jerk reaction to a specific problem in a specific situation that then has unintended consequences which become a larger issue than the original situation.

There are no cookie-cutter solutions or silver bullets to security problems. I wouldn’t deal with securing my home the same way if I lived in a house versus a condo versus a trailer versus a boat…well, you get the idea. Someone in the Lower Merion School District thought that the way to secure the laptops checked out to students was to install remote-controlled Web cameras. If the laptop were stolen, the Web camera could be engaged, and the identity of the thief would be known. This is one case where it would have been a good idea to step back and let others review this presumed simple solution for a simple problem. Had this been viewed through a wider-angle lens, the issue of privacy for students and their families at home would have come up. It wasn’t, and now there are lawsuits stemming from photos that were taken without the knowledge or consent of the students or their families: unintended consequences stemming from what someone thought was a good solution to a potential security problem.

As a CISSP (Certified Information Systems Security Professional), I was trained to look at issues from the 30,000-foot view. One of our key phrases is defense-in-depth. At its simplest, it says that counting on one level of security is not as good as multiple layers of security that are interrelated and well thought out. Let’s not forget as well that the best security measures don’t mean a thing if they don’t mesh with the policy and politics of your situation. My family once thought about getting a door/window alarm system for our house, but decided that the added benefits of owning an alarm system were more than offset by the additional requirements (remembering to set it, remembering how to turn it off in time and how to let the company know you didn’t turn it off in time, and other basic steps…), the layered security of our concerned neighborhood (polite way of saying nosy neighbors), and the noisy dogs. Would our house have had “better” security had we installed the alarm? Yes. Would our house have been more secure if we ended up just turning it off because it took too much effort to use it? No. It reminds me of something a buddy of mine used to say, “You can lead a horse to water, but you can’t make him bark.” Okay, maybe not…

A few years ago when I was transitioning between positions here at Washington University in St. Louis, I proposed we set up a Network Security Office (NSO). My experience with our residential students led me to believe that we needed a group looking at ways not only to protect us from threats on the Internet, but to also help protect the Internet from us. What we didn’t need was an overly technical group that would dictate solutions to our various schools and departments. We needed a group that could communicate with departments, listen to people’s security needs and help them take a larger view
of their particular issues, and allow them to see what others were doing on our campus and campuses across the globe. Working with fellow ACUTA members from both the academic side and our corporate partners helped me find models that worked well in situations similar to ours.

Over the years, the NSO has built up that very good reputation within the university. Even though I have moved away from responsibility for the NSO, I continue to routinely check out their website and use it as a source of information—both on what to look out for and good preventative steps to take. Feel free to check it out: http://nso.wustl.edu. You will find information about the latest phishing schemes, baseline information about securing individual systems, links to a top-ten security issues list, and a variety of other items.

Behind the communication effort, there are many technical efforts going on to help keep the campus safe from threats—both internal and external. The NSO has become a multifaceted organization that embodies the idea of defense-in-depth here at Washington University in St. Louis—an organization that will always “take a step back” before rushing into the fray.

One final note: ACUTA is always an excellent source of information on just about any telecom/IT topic. But you might want to make note, if network security is on your radar, that Track 1 of the Fall Seminar to be held in Vienna, Virginia, October 24–27 will focus on “Who’s in Charge of the Network?” I’m sure there will be plenty of very useful information available to attendees from campuses across North America, not just formally from presenters but in casual conversation with other attendees as well. I hope to see you there.
Report to the 2010 Annual Business Meeting

Each year, I have the pleasure of reporting to the Annual Business Meeting on some of the highlights of activities by the ACuta professional staff. For those who cannot attend, I would like to take this opportunity to share my report.

The ACUTA professional staff has had the opportunity to work on a number of exciting new projects during the past year.

Strategic Planning

This year, our strategic planning efforts were once again focused on working with committee and staff teams to implement the strategies and action items in the new Strategic Plan. The "Strategic Plan Report Card" was available at the Annual Business Meeting and posted on the Web at www.acuta.org/wcm/acuta/pdf/strategic_plan_report_card.pdf. It shows that of 62 total action items, 32 are already completed and ongoing, and 23 are under way. Our board, committees, and staff continued to refine the plan and develop new action items.

A major effort that is just getting under way is a focused strategic examination of ACUTA's educational and professional development offerings. This grew out of the work of the Event Schedule Task Force, which was charged with examining ACUTA's seminar and conference schedule, and evaluating the objectives, number, and types of events.

Committee Restructuring

I am pleased to report that in 2009, an unprecedented number of ACUTA members stepped up to volunteer to serve on our committees and subcommittees. We appreciate all of the energy and enthusiasm that our volunteers bring to the organization.

Continuing the work that was begun last year by the Committee Structure Task Force, this year we completed phase 1 of our new committee structure. Phase 2 is now beginning, with the planned introduction in 2010 of six new committees and subcommittees that will take on important responsibilities in the areas of environmental scanning, outreach, event development, online learning, and publications development.

All the new committees and subcommittees will have staff support to assist them in carrying out their responsibilities.

Information Technology Upgrades

We are in the final stages of a nearly year-long process of significantly upgrading ACUTA's technology infrastructure and services. Major systems, including our association management software and membership database, website, listserv, and back-office hardware and software, were all upgraded by March 2010. We have also introduced new social networking tools, the "ACUTA Community," which will provide online collaboration space for our committees and online discussion groups. Check it out at http://community.acuta.org/welcome.htm.

This technology upgrade has included a complete reexamination of our business processes and the introduction of new efficiencies in administration and financial procedures. It has been a major project that was skillfully led by Aaron Fuehrer, information technology manager, but in an organization the size of ACUTA it also touched and challenged every staff member. I would like to thank the entire staff for continuing their essential member service functions uninterrupted, while helping to shape, implement, and adjust to our new technology systems. I would also like to thank our board of directors for making this investment in ACUTA's future.
Public Policy and Regulatory Affairs

As the staff liaison to the Legislative/Regulatory Affairs Committee, I continued to spend a large percentage of my time monitoring and analyzing regulatory proposals and actions at the U.S. federal level, and working with the committee and legal counsel to plan our advocacy efforts.

Much of the focus this year has been in two areas: development of the FCC’s national broadband plan and implementation of the broadband stimulus grant and loan programs. ACUTA has been an active member of several coalitions of higher education and networking organizations, submitting comments and advocating for broadband services for anchor institutions including colleges and universities.

ACUTA continues to collaborate with other higher education and networking organizations on public policy issues, and this is reflected in a high-priority strategy in our Strategic Plan. Significant public policy collaboration partners included EDUCAUSE, Internet2, state research and education networks, research libraries, and other higher education organizations. These collaborations have continued to provide value to ACUTA members by helping us achieve our public policy goals.

We have also been able to provide several audio and Web seminars to ACUTA members on important public policy areas, such as the stimulus program, electronically stored information, and spectrum issues.

Collaborations

ACUTA members benefit from our collaboration with other organizations with common goals and values. In addition to our federal policy collaborations with EDUCAUSE, Internet2, and others mentioned above, we participated in the following collaborations:

- We collaborated with ITERA, the International Telecommunications Education and Research Association, by providing ACUTA judges for the association’s student case-study competition. We also invited participation by ITERA faculty and student members in our Unified Communications Summit in July 2009.
- We were active members of CHEMA, the Council of Higher Education Management Associations, participating in research projects and programs designed to improve communication among association leaders in higher education. The ACUTA president, president-elect, and I attended the CHEMA conference in May 2009, which provided valuable networking opportunities with officers of the other higher education associations.
- We arranged for NENA, the National Emergency Number Association, to provide an article for the ACUTA Journal.

All of these collaborations have been positive for ACUTA and our members, and we will continue to reach out to other professional and industry organizations with mutual interests.

ACUTA Conferences and Seminars

As reported last year, ACUTA conferences and seminars have not been immune to the effects of the widespread economic constraints at our member institutions. Registration at our events still has not returned to 2008 and prior levels, although beginning in winter 2010 we began to see a gradual improvement. Registrations for the Annual Conference and Strategic Leadership Forum were also higher than the previous year.

In order to meet the needs of members who were not able to attend our events in person, we offered remote access to our 2009–10 conference and seminars. We offered live and archived video streaming of the Unified Communications Summit in July 2009. Then, based on user feedback, we offered video of the fall and winter seminars on DVD. We continue to explore online options that offer meaningful educational content and are financially viable for ACUTA.

In addition, we offered a multi-event discount to ACUTA institutional members for 2010 events.

Economic Issues

Although we continue to face challenges as a result of budget issues at our member institutions, ACUTA remains on a secure financial foundation. We reached a milestone this year in completely paying off the mortgage on the ACUTA headquarters building, and it continues to be fully leased. In addition, our investments of reserves are performing well. The ACUTA board and staff continue to work to control expenses and develop new forms of revenue.

Conclusion

None of these actions could have been accomplished without the dedication and energy of every member of the ACUTA staff and volunteer leadership team. I would like to thank all the staff members for their professionalism and commitment to the continued success of ACUTA—and for the extra effort involved in successfully completing our technology upgrades. I would also like to thank our elected and volunteer leaders—our board of directors, committee chairs, and committee members—who continue to devote tremendous energy to guiding the association toward the accomplishment of its goals.

I’m sure we are all looking forward to a productive and successful 2010–11!
Cloud computing, hosting, managed services, anything as a service (xAAS) … The options for moving technology and technology management out-of-house (collectively referred to as “outsourcing”) are more numerous than ever. The claims about these services can be compelling, especially for an institution that is short on capital, dealing with personnel freezes and cutbacks, and facing replacement of obsolete technology. Since the question of whether to outsource technology services and support is being raised with increasing frequency at many colleges and universities, this article will provide the issues for consideration when determining how outsourcing best fits into an institution’s technology management strategy.

While complex, the range of options available for providing and supporting technology can be (over) simplified to a two-by-two matrix showing where the equipment is located as compared to who does the management. See Figure 1.

While the popular definition of outsourcing is presently “anything outside the firewall,” that definition is limited and doesn’t address contracted management of in-house assets. Outsourcing exists in quadrants 2, 3, and 4. Because the range of outsourcing options is so great, it appears that outsourcing is “taking over” from in-house management.

Thus there is a general perception among higher education senior management that many educational institutions are outsourcing their technology operations. (“Everybody’s doing it!”) This misconception arises from the fact that many institutions are outsourcing some technology services—for example, student e-mail. Outsourcers often take over some management aspects of the service, including equipment hosting, software support, marketing, and customer service. While some outsourcing is presently being done at many institutions (public and private, large and small), it is not at this time the prevalent management and service delivery option. I know of very few institutions where IT is totally outsourced.

Outsourcing has its place. It can be a cost-effective method of supplementing in-house capabilities, providing additional expertise, and allowing an organization to concentrate its limited resources on those efforts that best support its strategic mission. However, outsourcing is not an all-or-nothing decision. It can best be viewed as a continuum, moving from no outsourcing to full outsourcing. An organization must decide not only whether to outsource a function (IT, telecommunications, food services, custodial services), but often which specific tasks within that function to outsource.
Most of our clients believe that technology is too vital and too strategic to relinquish control entirely to a third party. However, many do outsource some technology services (maintenance, project management, cabling, consulting...). So, the question is not whether to outsource technology services—the question is what and how much to outsource.

**Why Is Outsourcing So Attractive?**

Outsourcing, in all its many forms, is increasing in popularity for many reasons. Chief among these are the following:

- Technology is increasingly complex, rapidly changing, and constantly converging. The speed at which most institutions budget and procure technology often leaves IT "behind the curve" and unable to respond as quickly as necessary.
- The flexible, scalable nature of outsourcing, such as being able to add or increase capabilities or capacity "on the fly," can be very attractive. Many cloud-based services can support this more easily than in-house services can.
- People are expensive, especially given the level of benefits at most institutions. In addition, complex hiring practices, remote locations, and lower pay scales impede the ability to find, attract, and retain the right personnel. With outsourcing, the number, type, and skills of support personnel are the outsourcer’s concern.
- Most (good) outsourced service providers have redundant, hardened data centers; redundant and diverse routing to improve business continuity; and a higher level of disaster preparedness. Using multiple services from various providers reduces the risk of a single, catastrophic failure. Replication of this same level of reliability on-site is expensive to provide and manage and may not address access in case of a campus disaster.
- Web-accessed, location-agnostic services appeal to an increasingly mobile population.
- Technology transitions are easier and technology is kept up-to-date with constant capital expenditures.
- Outsourcing is perceived as being "greener" (or at least the power consumption and carbon footprint fall to someone...
else). Space, power, and capacity planning for university data centers are all reduced.

It is important to note that outsourcing trends are cyclical. Various industries and functions alternate between outsourcing and in-house management. In the 1980s it was very popular to outsource computing functions, and companies like EDS and SCT made millions of dollars taking over computing departments. Throughout the '90s many institutions moved IT back in-house, citing higher costs, lack of flexibility, and lack of vendor responsiveness as the primary reasons. In the 30 years I have been an independent consultant to higher education, I've watched the outsourcing pendulum swing back and forth several times. Right now, we're strongly toward the outsourcing side, but many factors—including economic factors, changing technologies, and institutional attitudes—can affect the swing of the pendulum as well.

Issues When Considering Outsourcing

When technology is outsourced, numerous changes take place. It cannot be assumed that one can transparently make a transition of this magnitude without significant and sweeping changes in day-to-day operations. Changes include the following:

1. Contrary to popular belief, outsourcing doesn't eliminate the institution's need to manage; it just changes the nature and level of management. Someone still has to manage the outsourcers, the contract, the interface with the school, and so on. Failure to manage is the single most common cause of failure among outsourcing endeavors.
   - Control is lost, at least to some degree. No matter how good the management interface is or how responsive the organization is, control is no longer entirely yours.
   - Costs change, but don't necessarily decrease.

2. Your direct personnel costs are lowered.
   - No need to pay benefits.
   - There are fewer FTEs.
   - However, you will pay the outsourcer higher salary costs for comparable technology skills.

3. Recurring expenses may go down if the outsourcer provides more efficient service.

   4. "Free" services like Google Gmail tend to cloud the issue. (Pun intended.) While these services cost less on the surface, there are always the ultimate questions of how long these services will remain free and what "free" really costs.
   - Quality may improve or may suffer depending on how well you are currently doing things and how well the outsourcer will do them in the future.
   - Institutional knowledge is lost for outsourced functions.
   - Allegiance of staff is to the check signers. This is especially true with managed services where existing staff might be transferred to a third-party provider.
   - University technology is not generic. Every campus environment, infrastructure, network, and culture is unique. "Cookie-cutter" outsourcing organizations frequently don't understand this (at least initially).
   - Technology reaches every location, activity, and constituent of the institution. While certain functions can be easily segregated and outsourced, treating all of IT as if it were self-contained and able to be outsourced can be shortsighted and dangerous.
   - Technology is strategic to the institution. It is a fundamental, mission-critical function of the school. Outsourcers do not necessarily see it in this light.
   - Frequently, the principal difference between outsourcing and in-house services is where the equipment itself is located (your server room or the vendor's). But equipment location is only one piece of the technology puzzle. Outsourcing separates this piece and tries to deal with it out of the overall context.

   5. While outsourcers can frequently bring more and broader expertise to any given technology than is available from in-house personnel, in-house personnel often have a better feel for the culture and politics of the institution, which is valuable.
   - With the continued merging of voice, data, and video technologies and infrastructures, it is hard enough to coordinate the activities of internal staff for different departments. It may become even more complicated to manage these technologies when one or more of them are managed by an outsourcer.

Outsourcing Decision Criteria

Before you decide to outsource and to what degree, you should consider the following questions:

1. What problem are you trying to solve? Why do you want to outsource? Are you trying to save money? Improve service? Lower FTEs? Provide more or better service?

2. What does an outsourcer bring to the table that the institution does not already have in-house? (This should be asked up at the top.) Does outsourcing make sense in terms of the institution's stability, size, and culture?

3. Can the outsourcing company provide equal or better flexibility in terms of types and levels of service, hours of operation, and so on?

4. Which services make the most sense to consider for outsourcing? What would be the impact on staffing levels? Will the outsourcing company hire away some of your staff?

5. Is space allocation, together with all associated furniture and equipment, an issue in your organization? Would it be a factor in this decision? If the outsourcer is off-site, how far away is the company located?

6. How much control would you lose (or perhaps gain) by outsourcing?

7. How is performance measured? By whom?

8. What is your recourse if the outsourcing company is not working out? Are
There's never been a better time to change. To find new ways to connect. New ways to collaborate. New ways to share human knowledge, to work together, solve problems together, and bring the world a little closer. Together.

that's the human network effect

Visit www.cisco.com/go/education

welcome to the human network.
performance penalties and/or performance bonuses addressed in the contract? What is your exit strategy should you decide to not renew the agreement? Are there limits on price increases at the end of the contract term?

9. Is the outsourcer independent, or is it affiliated with a vendor? If the latter, how does this influence any decisions regarding selection of products and services for you? Is the outsourcer stable? Likely to merge? What would a merger do to your relationship?

10. What has been the experience of other organizations that have used an outsourcing company, especially this particular outsourcing company?

11. How does the outsourcer address disaster prevention and recovery?

12. What are the qualifications and experience of the employees that the outsourcer will provide? How is performance assessment and monitoring handled? What is your recourse if an outsourcer’s employee is not working out or if he or she leave the company?

13. How difficult will layoffs and reorganization be at your school? Are your employees unionized?

14. What are the pros and cons of having outsourced staff working with your staff and/or the staff of another outsourcing company?

15. How will customer service be handled? Will the change improve or degrade customer service on campus?

16. One attraction of outsourcing is that many of the outsourcing companies “aggregate” services from many different customers to achieve bigger discounts, and can negotiate bulk purchasing arrangements with suppliers. Will quality suffer when you become “a small fish in a bigger pond”?

17. How is security handled? Information security not only implies protection of personally identifiable information (PII) and data backup, but regulatory compliance and records retention as well.

18. Are there clearly spelled-out service level agreements defining the rights, responsibilities, and expectations of all parties? Are they fair and enforceable?

19. What changes need to be made to the campus IT infrastructure and WAN links to support the outsourced service with acceptable performance and reliability? Cloud-based and hosted services demand large, reliable pipes.

20. What about present assets and investments—can they be transferred to the outsourcer? Sold? Re-deployed?

21. How standard are the institution’s technology implementation and infrastructure? Do they lend themselves easily to outside services and management?

22. What about integration with other technology functions? Can the outsourced service interconnect and interoperate better with present and anticipated campus technologies?

23. To what extent does your outsourcing decision limit choices in the future?

24. What arrangements will allow you to sleep best at night?

Where to Start

If outsourcing is gaining traction at your campus and you are wondering where to start in your assessment, start with the areas where you are having trouble and are weakest. This increases the likelihood that outsourcing will solve real problems and provide a win-win for IT and your users. Any assessment of what to outsource and what to keep must start with a thorough understanding of the services you offer, what they really cost, their value to the institution, and the impact that moving them out would have on your department and your users. Only then can you effectively assess the options.

To understand what outsourcing will cost, financial modeling is a must. Evaluation of outsourcing options requires a traditional cost/risk/benefit analysis akin to the old “lease vs. buy” question. Things to factor into the modeling process include salaries, benefits (including holidays, vacation days, and sick days), training, test equipment, tools, computers, telephones, furniture, space—everything that relates to having an employee on the payroll as opposed to being on a contract and off-site.

The biggest caveat is to make sure that you keep people on your staff who are knowledgeable and experienced enough to properly interact with and supervise the outsourcer, question major decisions as appropriate, and be a liaison between the outsourcer and your own organization.

Summary

Colleges and universities are all about educating people. While technology services supporting that end must be provided intelligently and cost-effectively, human capital is ultimately more valuable than financial capital. Overall, long-term strategy generally favors a prudent balance of outsourcing and in-house management and varies from institution to institution.

Outsourcing has its strengths and its shortcomings. Outsourcing can work successfully for an institution in certain circumstances and for certain functions, but it cannot be viewed as an across-the-board cure-all for the ills that plague IT in higher education. Outsourcing must be carefully evaluated and weighed against issues such as control, the strategic value of technology to the institution, staffing, responsiveness, and, of course, costs. Properly applied, outsourcing offers many benefits; improperly applied, it offers even greater risks.

Careful assessment and thoughtful planning can make the difference between “a head in the clouds” and “ahead in the clouds.”

Geoffrey C. Tritsch is a vice president with Vantage Technology Consulting Group. He can be reached at geoffrey.tritsch@vantagecg.com.
Security: Prepare to Lose Some

Network security is like tennis. No matter how good you are—whether you are the Roger Federer or Venus Williams of network security—eventually someone is going to hit a ball past you. In fact, no matter how good your defenses are, somebody is going to win some games and might even win the occasional match.

Your job as an IT professional is to minimize the damage, adjust to the opposition, and keep your side in the game. Unlike tennis, IT’s net demands security in a game that will go on forever (see page 16).

All best practices should be adhered to for network security, including due diligence, malware protection, and access control. “Treat a college network the same as you would a business network and you will benefit both in protecting the college network and in introducing students who will be entering the job market to proper security practices and procedures,” says Frank T. Clark, senior product manager, Niksun.

“Colleges must take action,” agrees Adam T. Ferrero, executive director of network services with Temple University’s Computer Services group, Philadelphia, Pennsylvania. “We cannot sit back and hope for the best.

Like every college, Temple has a variety of users on its network. They range from students in their residence halls to computer labs, classrooms, faculty offices, administrative staff, and clinical areas. Each requires a balance of approaches.

“We must have enforceable policies requiring antivirus (AV) and proper patch management. Well-patched and AV-protected workstations don’t often cause trouble. The goal is to eliminate any unprotected machines from attaching to the network. Layering more protection on top of that just makes things all the better,” Ferrero states.

“It is important to make sure you have a handle on all your servers,” agrees Michael Wojcik, CISSP, a manager in the Global Services practice of Acumen Solutions. He notes that colleges have a significant amount of public and private IP address space and, for many, it probably isn’t allocated very efficiently or effectively.

On top of that, colleges are supposed to provide free and open exchange of information. “This inherently creates a unique challenge,” Wojcik continues. “It is important, however, to make sure you know where privacy and security are paramount concerns.” As an example, many universities have medical schools where information is protected by regulations such as HIPAA. Therefore, all information needs to be categorized according to its sensitivity and protected accordingly.

Because colleges cannot harden or control end-user workstations as a private company can, use of virtual local area networks (VLANs) is even more critical. “A good rule of thumb is to treat anything outside a protected VLAN as you would the public Internet,” Wojcik says.

Ferrero has deployed Blue Coat’s secure Web gateway technology for several years. “We have several Proxy SG appliances,” Ferrero continues. Currently, the number is at six. The seventh was a SG9000 beta test Temple participated in. “We just ordered
two SG9000s for ourselves," he continues. "We are also long-time Packeteer customers [they run two PacketShaper 10000s]. We use Blue Coat content filtering but no AV. However, that is only one of the many tools in his bag of tricks.

"We have several layers in play at this point," Ferrero says. "We have pushed AV clients to desktops aggressively (Symantec 11 on the university and McAfee at our health system). We have Blue Coat proxies protecting the labs and entire health system. By utilizing the content filtering, we very easily disable malware here."

Temple’s firewalls are Check Point VSX and IBM Proventia intrusion prevention. "The Proventia discards plenty of packets that match for problems," Ferrero says. After that, they have PacketShapers that are primarily tuned to discard peer-to-peer traffic signatures.

"The firewall rule set allows us to talk out but does not allow the Internet at large to talk in," he says. "We specifically define what services are available, and we keep it rather tight."

So, ICMP, HTTP, and HTTPS are all a user is able to get to on a Web server.

"We do our best to place all hosts/servers on firewall-routed networks such that from inside or outside the hosts are protected by IPS and firewall rules," Ferrero continues.

Firewall changes are reviewed by IT’s security team before implementation. "We typically deny any request for Internet access down to a workstation. Access is typically reserved for servers. We have found this mitigates the bulk of the threat," he states.

Colleges have to care for what is behind the firewall, too.

Beyond the basics, automatic, cost-effective protection—including long-term retention and destruction of data—is something that schools should examine. "Identifying what data have value and may need to be retained and protected is a critical component of the network environment at these universities and colleges," says Kamel Shaath, CTO at KOM Networks. It is important to comply with data protection laws, meet the basic needs of business continuity, serve users, and allow for reference material in conducting research.

Under data protection laws, colleges and universities are required to ensure that personal data are protected, secure, and accurate, Shaath says. Much of the data they hold cannot be held longer than is reasonable. But this is only one set of valuable data that needs to be protected and preserved, he notes. There is also scientific research, financial information, legal information, and so on, which may need to be held and protected for longer periods.

"Management and protected storage of valuable information should be the highest priority for any organization," Shaath continues.

A good start is automating the life-cycle management of data that need to be retained and protected. That means fitting an archive storage management solution into the existing environment without disrupting day-to-day operations and incurring the added expense of training, interfaces, and expensive connectors.

The place to start is leveraging existing storage, administrative talent, and knowledge.

---

**The Never-Ending Game**

Tennis matches go five sets. Football games last 60 minutes. The security game never ends. Experts agree that security is an endless, ongoing game—an expensive one.

Frank Clark compares it to maintaining a campus police department, fire department, or hospital. "Security is part of being a member of a global information network," he says.

Tom Claire agrees. "It is just another operational expense and it has been for years," he says. However, he notes that the cost, compared to most IT functions, is minimal. As a percent of a college’s IT budget, it usually is in the single digits.

Ferrero takes a common-sense approach. "Regarding firewall rules, we log everything we drop," he says. "We log as much access as we can. It has proven useful," he notes. There are spoofing filters on every subnet. "Every single subnet," he emphasizes. "It is the easiest thing to prevent IP spoofing and ensures packets can be back-tracked to their true source."

Still, Ferrero says, "I don’t see the end in sight. I’m not likely to stop locking my doors when I leave home anytime soon. Virtual desktop infrastructure and mobile devices change the requirements. But there is an ongoing need."

Unfortunately, security today is really an arms race, Wojcik says. "There are always new threats. Expenses are ongoing. Outsourcing as much as possible makes it possible to have an external provider, whose job is to provide security, to do the work. Of course, due diligence must be performed to ensure your outsourcer is competently handling your information," he adds.
Moving Forward

The need for security will only grow. “As distance learning grows and more students are not behind the gateway, the need for security will increase,” says Tom Claire, Blue Coat’s director of security product marketing. He predicts the biggest change colleges will see in the next year or two is in the amount of video and Web media that students and faculty will use.

Even beyond distance learning, this will include use of services like Hulu, which promises to outdistance cable TV. Claire notes that those watching the Olympic Games wanted to see a particular event—say all snowboarding events—and wanted to see it when they were ready…not when the network broadcast it. This trend, he predicts, will drive demand for IPv6 and will increase the need for transition gateways to handle video, “presence,” and live-based broadcasts. “Text is nice,” Claire says, “but humans are visual learners.”

All of those gateways—and everything behind them—will require protection. However, students and faculty are more vulnerable…they are impatient and like to multitask so may not pay attention as they skip from one link to another before stepping off the cliff. Phishing is at an all-time high, up 585 percent in Q3 2009, and cyber attacks have seen a five-fold increase in 2008–09 as compared to the past 15 years.

“Although not a security solution per se, many colleges are looking at things like IP address management (IPAM) solutions to help them keep track of their IP address space,” Wojcik says.

As a vendor, Claire says, “Our job is to provide a clean, compliant, safe Internet experience.” That holds for colleges or for companies.

There should be no real difference between the security posture of a business network and a college network, Clark maintains…no different than when securing any other network.

“Each network is unique in its design and requirements,” he says, noting that this is an important consideration to take into account when setting a security plan.

The old carpenter’s saying, Measure twice, cut once, “is just as vital in planning computer networks and their security as it is to a carpenter,” Clark says. “Security should never be an afterthought or something thrown in as an add-on after the network is built.”

Access control, physical security, data integrity, disaster recovery, and many other considerations must be taken into account at the same time as security. When Niksun designed the data network for its own new facility, Clark says they spent considerable time with legal, human resources, and facilities management as well as the IT department designing and planning long before anything was purchased or installed.

The Toolbox

Clark says there are two rather inexpensive tools available to every college: due diligence in end-user education and protection. “I cannot stress enough how this is a very important aspect of network security that is frequently overlooked. A facility can spend substantial amounts of time, money, and resources to secure a network only to be thwarted by a single user without AV protection, or someone who unknowingly follows malicious instructions received over the network,” he says.

“Ensuring compliance and updates with protective software along with education of end users against malicious communications is the first step down this road,” he continues.

 Infinity IS Soft Agent

- Ideally suited for agents that need to complete any type of call quickly and accurately
- Features a single point of focus with the amazing built-in search and action capabilities of the Soft Agent Sandbox
- Unique scripts guide your agents through the call process
- Offers seamless integrations with your existing PBX ACD
- Where your need it:
  - Help Desk • Alumni Fund Raising • ACD Agents
  - Switchboard Operators

Also available from 1Call: • IVR Speech Recognition • Voice Logging • Web-Based On-Call Scheduling and Directories • On-Site RED ALERT Rapid Response

Call (800)356-9148 today to find out more!
Continuous surveillance is the last step—the watchdog that never sleeps. “The need of the hour is egress filtering, lawful intercept, and constant recording of all network traffic with an eye toward any anomaly,” Clark says, noting that this continuous surveillance allows specific searches to be performed to ensure that no unauthorized information is leaving the network as well.

“We make every effort to place servers on our host subnets,” Ferrero says. They are firewall rule set and intrusion-prevention protected. Typical staff subnets have little restriction. They are publically addressed and can access the Internet directly. Computer labs are further protected with router filters.

“They are allowed to have Internet access via proxy server only,” Ferrero says. Temple’s health system areas are configured similarly, with Internet access through proxy server only.

The health system has another firewall with rule sets that allow only health system user networks to access their hosts. “We use router filters a lot,” Ferrero says. “We have environmental control systems that do not require Internet access or user access. So, we tighten the list of allowed communication as tight as we can get it. This requires a bit of management, but I believe it is worth the effort,” he adds. “We’ve gotten good at categorizing things appropriately so that the router filter rules are built from a template (rather than case by case as we used to do).”

You’re Going to Lose Some

Everyone and everything on campus or related to the campus should be seen as a target for the bad guys. Even the stereotypical penniless student’s checking account can be harvested for the pittance it holds. And a lot of students these days are not all that penniless.

“In addition to the security and privacy of student information (grades, bank account info), universities also have to protect the intellectual content on which curricula are built,” Wojcik says. In an era of increased distance learning and broadband technology, the security of this information also becomes a challenge. How best to protect? Or do you open some of your content intentionally as a recruiting tool or a community benefit?

While there are many precautions that can be taken, how far a school can take its security program is usually limited by budgetary concerns. Access control by way of one-time tokens, biometrics, encrypted VPN, and need-to-know restrictions, and network segmentation by way of VLAN are all available and excellent ways to protect sensitive data.

“Despite the best protection, security breaches occur all the time,” Clark says. “What is important after a breach has occurred is to contain the spread of the breach and to determine the exact method utilized and to implement countermeasures to ensure that it does not happen again.”

Products to Help

Technology solutions of all sorts are available. One company has an appliance-based scalable network security solution that integrates several critical security functions into a single architecture. It is a combina-

ACUTA Member Networks Are More Secure

An informal survey conducted in 2009 by ACUTA found that while a whole range of security threats continue to concern the people who run higher education computer and communications networks, they believe their networks are more secure than five years ago.

When it came to assessing the physical security of their networks, respondents to ACUTA’s survey expressed a high degree of confidence. Only about one in six survey respondents cited physical access as a potential security weak spot, instead seeing vulnerabilities such as mobile device usage and student downloads as much greater concerns. Also, in an overall ranking of the degree of danger that the various vulnerabilities might pose, physical access ranked below average, with threats such as viruses, phishing or vishing, and student hackers rated significantly higher.

In the ACUTA survey, 84 percent of respondents said they believe their campus networks are more secure now than five years ago, with six percent feeling less secure, and the remainder seeing no change. Asked to grade their own networks’ security, the aggregate response was a positive 3.7 on a scale of 1 (poor security) to 5 (best security).

The area of their networks that the largest percentage of respondents consider most vulnerable is usage of mobile devices. Thirty-five percent of respondents see these devices as a weak link in their security chain. Other top vulnerabilities are internal controls (named by 30 percent of respondents), student downloads (29 percent), student hackers (23 percent), and Internet access (20 percent). Physical access finished out of the top five, at 18 percent.

Physical security also finished sixth out of nine specific threats or weaknesses when it came to their overall “danger” rating. The most dangerous threats, ACUTA survey respondents said, were viruses and malware, unreliable internal controls, and phishing or vishing.
tion traffic-capturing, forensic-analysis, and security-reporting device that continuously surveys the network in real time and at line speeds to gather and analyze every packet on the network. Users are informed of security breaches, intrusions, anomalies, data leaks, and attacks as they occur.

According to the specs, it quickly answers questions such as how a breach occurred, what are the consequences of a hack, precisely what was compromised, who was affected, why it occurred, and how corrective measures may be initiated. It integrates both anomaly and intrusion detection into one platform to safeguard the network with fewer false positives. In addition to standard signature-based intrusion detection, it also monitors the network for user-defined and threshold-based anomalies.

Besides searching network application content for sensitive information, on the occurrence of an anomalous incident a security administrator has the option to reconstruct the application session within which the anomaly transpired.

Another company's solution is a scalable, hybrid architecture that combines two appliances with software and a cloud-based service to provide Web awareness and on-demand intelligence about the latest Web threats across the extended enterprise. The newest versions connect to the collaborative cloud defense service to obtain threat intelligence and Web awareness.

Other companies help clients (including universities) solve complex technology problems by offering innovative business-process solutions, strategy and technology know-how, and experienced personnel who achieve measurable results for the campus. They help clients weave cloud computing strategy and integration into the fabric of their existing enterprise architecture.

Best Practices

Whatever direction you take, Clark offers some best practices that will work at any college on any network. Some essentials are:

- Separate resources for the public-facing network (like the university website) and any systems that contain sensitive data
- Proactive protection from malicious traffic
- VLAN technology to establish need-to-know boundaries for the internal network
- Intelligent network design that takes into account future plans and network growth to ensure seamless expansion without costly downtime
- Regular patching and updates, to maintain both the security and productivity of the network
- Monitoring all software for changes and bug fixes along with maintaining support and licensing contracts for enterprise software
- Due diligence in monitoring—easy to implement but an often overlooked tool in the administrator's toolbox

No matter where in the game your school is playing, it is simply poor form to concede any points to the other side. Do the easy, inexpensive things first. That's like learning the basic shots. Add the tricky spins to your security portfolio as you go along. Soon, you'll be in the top flight of players—and the courtside bullies will go looking for someone else to pick on.

Curt Harler is a freelance writer and contributing editor for the ACUTA Journal. Reach him at curt@curtharler.com.

MiCTA – We Make Buying Easy!
515 N. Washington Ave.
Suite 405
Saginaw, MI 48607
Toll Free: 888-964-2227
www.mictatech.org

Offering Discounted Products

- Emergency Notification Systems
- Learning Management Systems
- Telecommunications
- Video Integrated Classrooms

MiCTA represents all nonprofit entities including educational, governmental, libraries, healthcare, religious, charitable, and public sector with members in all 50 states. MiCTA produces and publishes collaborative RFP’s generating agreements that are made available to all MiCTA members in good standing.
While the phrase may make for a funny punch line in a joke — it's part of the Down East humor culture of Maine — it is serious business for someone who aspires to become a Chief Information Officer. And a corollary to this for the newly minted CIO may be "I got here, now what?"

There is no clear path for technology leaders in higher education to follow when their goal is to become a CIO. In addition, depending upon their backgrounds, new CIOs often find themselves facing unexpected challenges with issues outside of strictly technical matters such as human resources and relationships with a board of directors.

It's for these reasons that Excelsior College has created the nonprofit Center for Technology Leadership, a resource to provide leadership training, mentoring, and networking for aspiring and current higher education CIOs.

A Potential Crisis on the Horizon

Over the past several years, Dr. Wayne Brown, vice president and CIO at Excelsior College, has been studying the role of the chief information officer in higher education settings. His research has revealed two very critical and related issues: looming retirements and preparedness of the next generation of senior leaders.

In his 2009 Higher Education Technology Leadership Study, Brown reported that 45 percent of higher education CIOs were planning to retire during the next 10 years (Figure 1. CIO Retirement Plans). This suggests that a significant number of opportunities will exist for technology leaders, in the next organizational layer down from a CIO, to move up to the top job. The pool of potential CIO candidates in this next layer is fairly broad which means that there could be stiff competition for those who are not well-prepared to make the move up the ladder.

Yet, among those in the next layer down — we will call them technology leaders or TLs — there are concerns about both the length and nature of their experience in the field. In his research, Brown has found that, as a whole, TLs have slightly fewer years of experience than might be expected when compared with current CIOs, and the mix of that experience is somewhat different than that which is reported by existing chief information officers.

The research, however, exposed a potentially serious threat to quality in the candidate pool of future CIOs, an important concern for search firms and hiring officers at colleges and universities. Among the TLs comprising the potential supply of CIO candidates, about 4 in 10 indicate
In contrast to the roles that a CIO is expected to perform, attributes are those characteristics and talents that distinguish one CIO from another. Most important, it is the extent to which an individual possesses and displays these attributes that determines how effective the CIO is in the eyes of supervisors and management colleagues.

that they are not interested in the top job or are themselves planning to retire within the next decade. Of the remaining, less than 3 in 5 technology leaders (56 percent) say they won't even begin a concerted effort toward becoming a CIO within the next three years. Another 41 percent, say they don't plan to start preparing for the CIO role for another four or more years.

Just one-fourth (26 percent) of TLs responding to the survey state that they hold positions that were specifically created to take over when the CIO was unavailable. Since there is no clear path for aspirants to follow in preparing for the CIO role, it follows that there is no understanding of the time it takes to acquire the necessary qualifications. Waiting to begin preparation will not only impact an individual's readiness to assume command in the short term, it lowers the depth of the replacement candidate pool for the CIO positions that will become vacant in the next few years.

Development of the next generation of chief information officers is clearly a significant issue. Yet, there is a present concern that may be less visible — but nevertheless essential — to the effectiveness of CIOs who are not retiring, especially those relatively new to the position. As top leaders leave the field, there will be fewer experienced individuals on whom those remaining on the job can rely for guidance, advice and problem solving. Peer networking and support has been found to be a highly important element in the CIO's success tool box.

What Does it Take to Be a CIO?

In a companion study of the roles and effectiveness of chief information officers in higher education (Brown, 2009) both current CIOs and colleagues who are members of the management team at the same institution were surveyed. The various roles that a CIO plays were identified as shown in the chart below.

Higher education CIOs and their management colleagues appear to have fundamental agreement on the basic roles that CIOs are expected to play and on the level of importance

Figure 2. CIO Roles

<table>
<thead>
<tr>
<th>CIO Roles</th>
<th>Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Partner →</td>
<td>Organizational strategic planning and revising business processes</td>
</tr>
<tr>
<td>Provider →</td>
<td>Foundation of IT support and responsive department</td>
</tr>
<tr>
<td>Contract Oversight →</td>
<td>Relationships with IT vendors, contract negotiation, and contract supervision</td>
</tr>
<tr>
<td>IT Strategist →</td>
<td>Ensure security and accuracy of institutional data and alignment of IT department with the institution</td>
</tr>
<tr>
<td>Integrator →</td>
<td>Integration of all internal and external systems</td>
</tr>
<tr>
<td>IT Educator →</td>
<td>Evangelist for computer use and understanding Educator of employees on how IT innovations bring value to the organization</td>
</tr>
</tbody>
</table>
these roles have at their respective institutions. For example, both groups rank being a classic IT support provider and serving as an overseer of IT-related contracts as foundational CIO roles. They also agree that being a business partner and an IT educator are the least important among CIO roles.

As might be expected, there are variations in the titles, age, gender and reporting relationships of CIOs depending upon the size of the institution. There are also variations among the fields in which CIOs have earned their academic credentials. There is strong evidence that CIO candidates without an advanced degree may have limited growth prospects.

What is quite telling among all the research results, from both 2009 and preceding years, is a set of attributes that describe the successful CIO. In contrast to the roles that a CIO is expected to perform, attributes are those characteristics and talents that distinguish one CIO from another. Most important, it is the extent to which an individual possesses and displays these attributes that determines how effective the CIO is in the eyes of supervisors and management colleagues.

For CIOs by CIOs

The Center for Technology Leadership at Excelsior College has been established to help aspiring higher education CIOs, and those already in the job, to better understand the duties they will be expected to perform and to help put them on a path toward developing the attributes that make CIOs successful.

First and foremost, The Center is a resource built by CIOs for CIOs. The executive director, Wayne A. Brown, a longtime CIO with a PhD in educational computing, is vice president for information technology at Excelsior College. Founded in 1971, this private, nonprofit college has been a national leader in distance education for nearly four decades. Accredited by the Middle States Commission on Higher Education, Excelsior has enabled more than 131,000 working adults to earn degrees and gain skills, giving them the flexibility to balance work, school, and family obligations.

A distinguishing feature of The Center is its advisory board which includes some of the nation’s most experienced higher education practitioners. These successful leaders represent colleges and universities of varying types and sizes: public and private, small and large. They know what it takes to be successful in the position because they live it every day. And they are not just advisors to The Center. They are also the industry’s finest who deliver its programs.

---

**Figure 3. CIO Attributes**

<table>
<thead>
<tr>
<th>CIO Attributes</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Communication</td>
<td>• Fluent in business language&lt;br&gt;• Fluent in higher education language&lt;br&gt;• Able to communicate and present information without technical terms</td>
</tr>
<tr>
<td>IT Knowledge</td>
<td>• Fluent in business language&lt;br&gt;• Fluent in higher education language&lt;br&gt;• Able to communicate and present information without technical terms&lt;br&gt;• Fluent in business language</td>
</tr>
<tr>
<td>Political Savvy</td>
<td>• Able to assess situations that might be confrontational and act tactfully&lt;br&gt;• Able to work well with a majority of people</td>
</tr>
<tr>
<td>Strategic Business Knowledge</td>
<td>• Knowledge of institutional offerings&lt;br&gt;• Understanding of market and business processes&lt;br&gt;• Familiar with the competition</td>
</tr>
</tbody>
</table>
The Center Offers Two Intensive, Five-Day Courses

Technology Leadership: A Foundation for Aspiring Higher Education Chief Information Officers

Designed for those individuals who are in higher education technology management positions and who are thinking about advancing their career path, this 5-day course comprises a broad range of key subjects:

- IT and higher education issues
- Security and compliance
- Technology governance
- Strategic planning
- Policy and ethics
- Financial planning
- Leadership
- Roles of a higher education CIO
- Career preparedness

Leadership and the Higher Education Chief Information Officer

Designed for collegiate CIOs who have been in this critical leadership position for five years or less, this 5-day course includes a wide variety of key topics:

- Executive and board interaction
- Finance and budget
- Human resources
- Leadership
- Networking and professional development
- Roles of a higher education CIO
- Strategic planning
- Technology governance
- Communication

Becoming and staying successful as CIO takes more than just an intensive course and it doesn’t happen in a vacuum. When students participate in a course from The Center, they move along as a group, learning concepts and grappling with exercises collaboratively. As a result, the contacts they make are contacts for life. Afterward, each course comes with six hours of advising from some of the nation’s foremost collegiate CIOs to help students smoothly navigate through even the thorniest of challenges. Additional advising is always available.

Center Membership

The Center’s programs are designed with the individual in mind. Institutions of higher education, and the businesses and associations that support them, are welcome to become a member of The Center. Because they have a direct stake in the development and availability of a pool of qualified CIO candidates, these organizations can benefit in a number of ways. Among them is reduced tuition for their employees who participate in programs offered by The Center. Other benefits include:

- Access to proprietary research
- Job advertisements
- Publications on issues and trends
- Industry news and updates
- Discounts on consulting services

Start on the Path to CIO Success Today

For more information on the Center for Technology Leadership at Excelsior College, visit our Web page at CTL.excelsior.edu or email us at CTL@excelsior.edu.

The Center for Technology Leadership at Excelsior College Advisory Board Members and their Affiliations

<table>
<thead>
<tr>
<th>Name</th>
<th>Affiliation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sharon E. Blanton</td>
<td>Chief Information Officer, Portland State University</td>
</tr>
<tr>
<td>Timothy M. Chester</td>
<td>Vice Provost and Chief Information Officer, Pepperdine University</td>
</tr>
<tr>
<td>Mitchel W. Davis</td>
<td>Chief Information Officer, Bowdoin College</td>
</tr>
<tr>
<td>Lawrence J. Haffner</td>
<td>Vice President, Information Technology, Webster University</td>
</tr>
<tr>
<td>Joy A. Hatch</td>
<td>Vice Chancellor for Information Technology Services, Virginia Community College System</td>
</tr>
<tr>
<td>Gren Hayes</td>
<td>Vice President of Services, SunGard Higher Education</td>
</tr>
<tr>
<td>Mary Lou Hines Fritts</td>
<td>Vice Provost and Chief Information Officer, University of Missouri-Kansas City</td>
</tr>
<tr>
<td>George Kahkedjian</td>
<td>Chief Information Officer and Vice Chancellor, Connecticut State University System</td>
</tr>
<tr>
<td>J. Craig Klimczak</td>
<td>Vice Chancellor for Technology and Educational Support Services, Saint Louis Community College</td>
</tr>
<tr>
<td>Polley Ann McClure</td>
<td>Vice President for Information Technology and Professor Emeritus, Cornell University</td>
</tr>
<tr>
<td>Gordon D. Wishon</td>
<td>Higher Education Consultant</td>
</tr>
</tbody>
</table>

Advertorial
Mobile Security in the Middle

As we become increasingly mobile, our data access goes with us on a bewildering variety of mobile computing and communication devices. The increased convenience and efficiency make the siren call of these devices nearly impossible to resist. They keep us connected and allow us to work and play anywhere, anytime. All, however, is not sunshine and blue skies.

Shadows lurk at the periphery of the colorful glowing wonder of all this access; loss of data, inadvertent release of information, and outright theft of data. These threats and losses are very real and can be very expensive to pay for and to prevent. There are at least four technological approaches to securing the ends of the process, and a fifth dynamic in the middle.

Technological Approaches to Data Protection Involve Four Basic Dynamics

First and most visible are software protections. Initially, fighting against malicious virus code was the mainstay for protecting computers and networks, but it is now only one tool in the arsenal. Threats now come in the guise of adware, spam, and inopportune Web downloads. Intrusion systems and firewalls provide additional security. Protective software provides a shield against basic threats but cannot do the job alone.

Second is authentication, providing essential assurance for both the server and the served that their connection is a trusted one. Many modern systems require both an informational key (a password or pass phrase) and a physical key (a key card or fingerprint reader).

Third is strong encryption of the data in transit. If the data stream is intercepted, without the encryption key the thief cannot read the content. However, if the thief has either the key or the device in hand, the door is open.

The final step, data backup, is often forgotten, especially on mobile devices such as laptops, netbooks, and smart phones. Some mobile protective systems have the capacity to wipe the memory of a lost or stolen device. However, if the data on board are not backed up, they are lost forever.

This Covers Both Ends of the Process, but What About the Middle?

There is a fifth, non-technological dynamic to consider: the interaction of people and security policies. Protective software is less effective if not updated, and useless if not installed. Authentication (usually a password) is less effective if shared, written down, or weak. Encryption slows down mobile devices, making this an enticing step to skip. Backup is often simply forgotten or ignored. How do you strengthen this “fifth dynamic” in the security process?

Justin Ragsdale, director of network operations, division of technology services at Wentworth Institute of Technology, and Matthew K. Arthur, director, incident communications solutions, information services and technology at Washington University in St. Louis, provided answers to four pointed questions. These schools are very diverse: Wentworth Institute of Technology is a small school, with about 3,600 students. Washington University is much larger (about 13,000 students). Please keep this in mind as you read their responses.
Question: Have the problems grown so diverse and the options so great that centralized security solutions can no longer be effective?

Matt: I would have to say that the problems have always been diverse and centralized security solutions have rarely been the answer (or effective). “Defense-in-depth” is a phrase that is commonly used within IT by those responsible for security and privacy. That being said, technology is rarely the “solution”—but more often a means to accomplish or assist with university policy.

Universities are, by their nature, very diverse with different technology support layers that rarely work universally. One school/department within the university might take some measure to comply with university policy that is totally different from the approach of another school/department. We have chosen to provide some enterprise-level IT security services (edge intrusion detection, basic internal scans, and others), but leave it up to departmental desktop support to assure installation and update of patches, antivirus, and so on. One interesting development: Having a respected network security office helps the school/department IT folks make more robust changes since they can “blame it on the network security folks.”

Justin: I would say that centralized security solutions still play a very important role in the network infrastructure. Will this start to change in the coming years? Probably, but for most institutions, a centralized approach will be necessary for the environment in which we live and work. Unlike professional environments that can have strict desktop/laptop policies (where users are not administrators of their computers), in the education environment this is usually not the case. This creates a strong need to centrally control the policies on computers and security solutions.

I’m not sure I would say the problems have become so diverse; if anything, they might be more contained. It’s the effect that these problems cause that has grown and will be the future driving force.

Question: Is the solution for the central security providers to work with individual users, recognizing their central role in maintaining security?

Matt: If by “individual users” you are referring to the school/department IT support folks, then yes. We have more than 12,000 students, 15,000 staff/faculty, and six campuses. There is no way our network security office could ever “effectually” reach out to that many individuals.

Justin: Yes. There is only so much that security products can do. Awareness is just as important, if not more important, than the actual products that are installed locally and at the core. Having the individual users as the first line of defense will aid in the protection of the data. As IT members we are not the owners of the data, we simply provide efficient and effective methods to access the data. The end users need to be aware of the importance of data security.

Question: What is your college or university doing to work with the users?

Matt: Mostly [we have] programs aimed at students via our student technology ser-
vices office, which provides documentation, training, and support to our residential population directly and all students indirectly. See STS Safe Computing: http://sts.wustl.edu/sts/index.php?option=com_content&view=article&id=82&Itemid=66

The school/department IT support folks reach out to individual users as appropriate.

Justin: Recently the Massachusetts government passed new laws that require educational institutions to have plans in place regarding how they are handling PII [personally identifiable information] data on the campus, as well as dictating that any PII data that leave the campus on a mobile device be encrypted. IT is not leading this initiative but is at the forefront of many of the decisions and solutions. Prior to this, many users did not look at security as part of their job description or have a full understanding regarding the scope. Within our IT department, we have officially created a security compliance team responsible for gathering data regarding systems security, identifying risk, identifying solutions, and providing guidance to other departments. Other departments are creating similar committees.

For the public in general, we plan to increase the number of campaigns (e-mail blasts, posters, information sessions) to end users to increase awareness regarding desktop/laptop security and data security. Currently, these announcements are only made in response to an incident, but going forward we will be doing them at strategic times during the year. In addition, we will be increasing the level of security features on the desktops. This includes such measures as screen-saver lockouts, stricter password rules, installing encryption software, moving people's desktops into a virtual environment, and potentially other measures.

There have also been talks about doing official security training for those people who have been identified as having access to PII data.

Question: Where do you think increasingly limited dollars for security should be spent?

Matt: Your comments about data and mobility strike a chord. Our smartphones on campus recently started requiring a four-digit password after a certain number of seconds of non-activity or when starting up. This was a minor change to the BES (Blackberry Enterprise Server) in response to new policy clarification.

I would like to see more dollars following data and mobility. For example, our medical school has started providing two-factor authentication thumb drives (finger-print and password). We need to spend more effort on laptops in particular to assure encryption, and so on. However, that won't happen without clearer guidance from university policy.

Justin: Identity lifecycle management (ILM) software. The questions that people should be asking are: Do you know who has access to your data? Do people who no longer work at your institute still have access to your data? Do they have an account? When people move from one department to another, is there a formal process for changing their access rights? How often is this reviewed, and who reviews it? All of these questions can be answered if you have ILM. Can the department/division heads run real-time audits against who has access to their data? What was normally an IT operation should be moved to the division/departement level. Increasing visibility into system access will help people understand that they can control the environment.

Conclusion

Comments from Justin Ragsdale summarized the situation very well.

"When it comes to security, I think that you really need to increase awareness of what it means and how the users can help. Because it is talked about all the time, some of the basics have eluded people. Common sense is still sometimes the best solution. A lot of people think, 'Oh, IT has us secured.' In reality, IT can only secure data and endpoints to an extent. We would love to keep data all in one location, with very limited access rights, but doing this decreases the value of the data and ultimately alienates those you serve.

"With the increasing number and variety of mobile devices in our environments that are usually not under IT’s control, end users need to understand the risk. IT also needs to adapt to the new technologies and allow users to access data through more devices in a secure manner. The amount and use of mobile devices is one of the main driving forces behind security initiatives. While security initiatives are mainly reactive, I think that IT application and mobile developers need to develop mobile access directly into the initial design stage of services. Instead of thinking, 'Okay, now that we have this application, how can we make it mobile?' they should make it mobile to begin with. This will help to ensure that the same security initiated for the application/service is applied to the mobile app/access."

Thanks to Justin Ragsdale and Matt Arthur for sharing their insights into mobile security issues. Although technology can provide security at both ends of the process, the people in the middle are crucial to the protection of critical data. Large or small, institutions must acknowledge the critical role of the user. The users must know what is needed and what is expected as part of the team safeguarding their own and their institution's data. With greater freedom comes greater responsibility.

Elwin (Mick) McKellar is a freelance writer and professional archivist who regularly contributes to the ACUTA Journal from his home in Michigan's Upper Peninsula. Reach him at mick@pasty.net.
Thanks to all the companies that support ACUTA as Corporate Affiliates!

Year after year, our Corporate Affiliates provide meaningful support to the association and its members as they contribute valuable information in sessions, in our publications, and on the listserv; provide personal attention and excellent customer service; and participate in our events by presenting, exhibiting, sponsoring, and attending. As you have need of various products and services, we encourage you to include ACUTA Corporate Affiliates in your RFI/RFP solicitations. (Note: List of members as of 5/4/10)
Things You Might (or Might Not) Know About Convergence Planning

Organizing planning and funding requests is an important part of a campus's transition to convergence technologies. Generally, technology convergence refers to combining voice, data, and video services onto the institution's data network. In the context of unified communications, convergence also includes messaging (e.g., voicemail, e-mail, IM, and fax) and collaboration (e.g., screen sharing and whiteboarding) channels. It's a centralization of services that, on the face of it, should create cost savings; technical and operational efficiencies; and a better, easier-to-manage IT environment. Well, maybe so, maybe not. It all depends on your specific situation.

Being able to present and justify relevant information on your convergence project will greatly aid your requests for funding. Analyzing convergence requires consideration of a number of complex issues, including technical, financial, and organizational issues, user issues, and planning issues—and something that overlays all of these, and is often not clearly considered: political issues. The institutional politics surrounding all of these issues plays a role, like it or not.

Politics

Let's talk a little about politics before getting into the more obvious aspects of convergence. Institutional politics has to be considered in any discussion that impacts the technologies that keep your college or university running.

So question number one is: As a CIO or a senior IT director, what is your place in the institutional hierarchy? Are you reporting at a level high enough in your administration to be effectively heard? If not, take that into consideration when planning for change. IT is a strategic resource, and if it's not considered one by senior administration, you have an important political issue that needs to be considered and dealt with. It can and will have a significant impact on what needs to be done versus what actually gets done.

Institutionally, who gets what financial resources is a political issue. How much should be spent on technology when there are other academic priorities that may be starving? What's the best way to fund technology so that it's not only sustained but improved going forward? How can your organization be expected to provide first-rate services if you don't have authority to hire and train the right people? These are all important political issues that play into the mix. To the extent necessary, they need to be brought to the table and discussed openly.

Technology

At the most basic level, technology-wise you need to look at such things as existing hardware and electronics along with the software that makes the systems work, their age and condition, and how well they serve your needs. What would best replace them, and how would this new hardware and software function? This, of course, refers to all of your systems—voice, video, computing, and network systems (both wired and wireless).
It also includes the infrastructure your systems run on: the inside and outside cable and wire plant, its pathway (conduit, duct banks, and manholes) and the technology closets that house cable distribution as well as electronics and their support systems (HVAC, power, etc.). The condition of distribution closets is often the most complex and costly aspect of the entire convergence effort.

Organizational Issues
You’ve probably heard “technology is easy: managing it is hard.” Dealing with the organizational issues that come along with convergence can be very troublesome—and not just in the short term.

Converged systems work differently than the systems we’re used to, with the emphasis being on the data network. The most common and obvious example of this comes when your tried-and-true PBX becomes “just another application” on your data network. Everything changes: perceptions of the importance of voice service and how it’s used, service delivery techniques and options, required skill sets, and organizational hierarchies. Plus, egos can, and often do, clash.

These issues are also true to one degree or another in how computing and video services are managed and delivered. In the former, consolidating databases, sharing information, and improved collaboration are extremely desirable. But management and maintenance become much more complex.

The same is true with video applications—and there are many of them, ranging from “simple” entertainment offerings, to video teleconferencing, to classroom and distance-learning applications. And don’t forget the variety of security applications that offer management challenges ranging from who manages what to all of the legal and privacy implications involved.

To some degree all of these management issues currently exist, but with convergence they will be dealt with differently; in fact, they must be dealt with differently if you expect to enjoy the full benefits of convergence.
User Issues

Your users shouldn't become the victims of all the good things that convergence will bring. Generally speaking, and as good providers of IT services, you should have an accurate feel for how satisfied your user community is with your current systems and services.

More specifically, you should have a feel for the specific sore points that exist. Not enough features in your telephone system? Too many competing databases to contend with in your computing systems? Are there bottlenecks in your network that sometimes slow everything down? Students getting tired of Lawrence Welk reruns?

At a different level, are your users demanding services you know they need but you can't provide? Or are they looking for things that you know, in your heart of hearts, they don't need? Are they—or worse, is senior management—driving you crazy with the latest fad of the moment drawn from this month's issue of their favorite airline magazine?

Finance and the Budget

Money and how to get it is, of course, the most important issue of all, and it's one of the drivers of this article. Having a good handle on your current finances is critical if you're going to succeed.

What are your current operational costs? Capital costs? How much are you spending to refresh and update hardware and software in each of these systems? Is system refresh being done on a regular systematic schedule? (Let's hope.) How much are you spending on your cable plant and pathway infrastructure each year, and what's the outlook for the future of these expensive systems? And where is this money coming from? Annual appropriations from your institution? User fees? Grants and contracts? Debt? How stable is this income?

And the beat goes on. What is your sunk investment? That is, what do you (i.e., your budget and/or your institution's) still owe on these systems? Are all of your systems fully paid for, or is there significant debt service still to be retired? Unless you're willing to write off existing debt, the cost for convergence can be tough to justify. New systems have new costs associated with them, some not obvious until a full analysis is done. A key element of your planning process is the financial analysis that will justify the cost of new systems.

Don't forget to count soft and hard dollar savings, especially as a technological solution may pay for itself over some period of time. Presence and mobility elements of a unified communications solution, for example, often have very short payback periods.

Planning Issues

It's probably fair to say that you have a pretty good handle on a lot of this, but it's also probably fair to say that some of it keeps you tossing and turning at night sometimes. This is where good and comprehensive planning comes in.

You can't implement a comprehensive convergence plan all at once, even if you think you have the energy and the skills to do it. It's too complicated, and circumstances change too quickly. Notice we didn't say technology changes too quickly. Everyone knows that, and it's mentioned constantly for one reason or another.

The fact is, all of these things change too fast. One day you're rich, the next day the bottom has fallen out. The president has suddenly resigned and the new one has a completely different perspective and agenda. Your PBX vendor just sent a letter telling you they're not going to support your voice system after next year. An air conditioner went out last Friday night, and by Sunday afternoon an entire network hub was cooked before anyone noticed. Oh, and technology is changing really fast too.

The planning for all these things needs to be started in terms of an overall, general review of all your systems and services, based on the issues discussed above. What are their strengths and weaknesses, and what are the logical priorities that should be set in place to guide the order in which things will be done? Maybe you know all of this already—it's all in your head, but it needs to be put into a formal plan that's understood and agreed to by senior management.

Summary

Let's summarize by identifying the essentials. To obtain funding there are three basic things to accomplish. Develop your case, establish your expertise, and sell it to senior management. In doing so, keep the following in mind:

1. Politics: Think about your position and role in the administration of the institution. To whom do you report, and is IT considered a strategic resource? If not, talk seriously about this with your superiors. Like it or not, IT systems and services must be treated as a strategic resource. IT is too important and too expensive, and its management is too complicated to be treated otherwise.

2. Analysis: Look at all of your systems and services with a jaundiced eye—one that takes into consideration the following issues:
   - The age and the usefulness of each technology and service and their importance and applicability to your users
   - The impact that changing the technology or service will have on those users and your institution
• The impact that it will have on your organization and how the new system(s) will be managed.
• The short- and long-term financial ramifications of the needed changes (both capital and operational) over the life of the system. Again, it's not just about cost, but also about the bottom line. Revenue (top line) increases are possible. Cost savings are possible as well, through improved efficiency and productivity, enhanced communications and collaboration, shorter time to market/solution/resolution, and so on.

3. Prioritization: Prioritize the work to be done and determine generally how the upgrades or replacements can best be accomplished to ensure an optimum IT environment now and in the future. (Notice the term "optimum IT environment," not "optimum converged environment." Chances are it will be converged in the long term, but you must do what's best in the short and medium term also. And you must do what's best for your institution, not what some smart guy outside thinks is best for your institution.)

4. Plan: It is extremely important that senior management see IT as a strategic resource in running the institution. From your analysis and prioritization, develop an overall strategy and plan for discussion, buy-in, and approval of senior management:
• Make senior management part of the ongoing process.
• Develop their understanding of the issues and gain their support.
• Make them contributors to the plan.
• Give them a stake in the work to be accomplished.

Conclusion

Sound easy? It's not. The transition to convergence takes careful planning for successful results. It is also a critical activity to secure approval of budget requests and adequate funding. And beyond that there's a number five to add to our list above:

5. Specific plans: Based on your priorities, take the systems and services that need attention first. Perform a specific, detailed assessment that takes into consideration and fine-tunes the issues developed above. From this accomplish the following steps:
• Review and select potential vendors and/or service providers.
• Develop a detailed request for proposal (RFP) document.
• Distribute to selected vendors/service providers.
• Manage the process (question period, on-site meetings, campus tours, and so on).
• Analyze responses and select vendors/service providers.
• Negotiate appropriate contracts.
• Implement.

Don't forget to maintain a long-term view and build in a high level of flexibility: Change is constant.

Mike Grunder, past president of ACUTA, is a consultant with Vantage Technology Consulting Group. He can be reached at michael.grunder@vantagetcg.com.

Paul Kirvan is a freelance writer who specializes in technology topics. He can be reached at pkirvan@msn.com.

Innovative Networks for Inventive Minds

As the top U.S. holder of optical patents, we know the value of education and research. We also understand how the right network infrastructure enhances communications and learning.

As your network solutions architect, we'll get involved, design to your needs, and help you develop a network to serve tomorrow's brightest intellects. Talk with us about how we can work together.

http://us.fujitsu.com/telecom
800.777.FAST (3278)

©2010 FUJITSU (and design) is a trademark of Fujitsu Limited. All Rights Reserved.
Reviewing the Lessons from Security 101

Janet A. Hutton

Back in December, Virginia Bentley, director of telecom services at Illinois Institute of Technology (IIT), posted a message to the ACUTA listserv. IIT was being flooded with calls from cell phone users around the country who saw that one of IIT’s DIDs had called them, but the caller left no message in their voicemail. So they called IIT (the DID) to ask who had called, and the group assigned the DID was being overwhelmed.

"After a time," says Bentley, "we disconnected the DID, which sends a caller to an announcement in our G3R that says: 'You have reached an unidentified extension at Illinois Institute of Technology. Please hang up and dial the main number [spoken number] for further assistance.'

"The major flood of calls has stopped, but we get one or two a day. However, these are harassment calls for which we could erroneously be blamed. We considered putting a voice mailbox on the DID with a special message. The preferred solution is to find out who is placing nationwide calls to people's cell phones ... and report them to the authorities."

Bentley says she even googled the DID to see if a company had posted it on the Internet as their number. She found "a few websites that listed a complaint against the number and described what I did here, but I do not know who polices those sites. It also looks like this is a widespread problem with other numbers."

Bentley might also have suggested that call recipients contact their telecom office to have their lines monitored to determine the "actual" origin of the call (if, in fact, someone was masking their number with IIT's DID). Someone might also have been accessing dial tone off IIT's PBX. Putting a mailbox on the DID and encouraging the caller to leave a message would allow the telecom office to run CDR from the local voice messaging system and determine the actual origin of the call. Bottom line: This is a security issue, and security is an issue we all must address.

Stopping the Hackers

When I think of systems security, what first comes to mind is hackers. We all know what a hacker is—it's someone accessing another person's computer without authorization, or gaining unauthorized access to a computer system or data belonging to someone else. Hackers are usually computer enthusiasts, typically skilled in computer technology and programming but lacking in ethics.

As a manager of voice messaging systems, I am always concerned about enabling the appropriate protocols to prevent the system from being hacked. For example, we change passwords frequently, and ensure that passwords are not obvious and don't start with "0." We change the system manager password when a system administrator leaves the organization. We are focused on setting our system parameters to secure our system and prevent any external forces from gaining access.

In years past, direct inward system access (DISA) was feared as a hazardous entry point for potential hackers. DISA is a PBX feature by which a caller, upon entering a code through a touch-tone phone, gets another dial tone for accessing some or all of the features of the PBX, such as making an overseas call or leaving a voicemail message.
When I worked as senior telecommunications coordinator in the pharmaceutical industry, my boss cautioned us about DISA, although we still used the feature (with a secure access code) to set up for remote workers during our telecommuting pilot program. Recently, I asked Vincent LaPrete, Princeton’s SL-100 switch programmer, for his thoughts on DISA and how applicable (or not) that feature is today. He replied:

“Over the last decade, the use of direct inward system access has decreased dramatically, and rightfully so. DISA has always been looked at as a risky proposition at best due to the system vulnerabilities that it creates. Some companies still use it as a means of allowing remote or traveling users access into the company’s phone system to make long-distance calls rather than dealing with supplying calling cards or cell phones. This trend has been reduced because of the practicality of cell phones.

“DISA can be a useful tool, and still has some specific uses today. We do use it currently on a very limited basis and have very strong password restrictions in place as hackers have long seen it as a weak link into a target’s phone system. If someone were to use it today, we would suggest starting with a strong password policy, including obscure passwords, changing them regularly, diligently monitoring accounts, and deleting unused accounts in a timely manner. If DISA is not being used on your system, we suggest having it removed from your PBX.

“All in all, we believe that DISA still has specific merits when diligently monitored, but with the other options available today, we might choose to avoid it.”

SECURING THE USERS

The Federal Communications Commission describes measures for voicemail subscribers to prevent hackers from dropping dial tone or placing calls from a voice messaging system as follows:

- Always change the default password from the one provided by the voicemail vendor.
- Choose a complex voicemail password of at least six digits, making it more difficult for a hacker to detect.
- Change your voicemail password frequently.
- Don’t use obvious passwords such as an address, birth date, phone number, or repeating or successive numbers (i.e. 000000, 123456).
- Check your recorded announcement regularly to ensure the greeting is indeed yours. Hackers tend to attack voicemail boxes at the start of weekends or holidays.
- Consider blocking international calls, if possible.
- Consider disabling the remote notification, auto-attendant, call-forwarding, and out-paging capabilities of voice mail if these features are not used. (www.fcc.gov/cgb/consumerfacts/voicemailfraud.html).

CONCLUSION

Our campuses are by nature very vulnerable. We have a mandate to make information available, but we are challenged to protect our users—including faculty, staff, and students. It is imperative that we remember the basics as we consider not only how we can enhance our system security but how our system can enhance security for our people.

Janet Hutton is the manager of voice messaging systems at Princeton University. Reach her at hutton@princeton.edu.
How Universities Can Persevere in the Security Marathon

Dave Durbin

Data theft is a constant threat in universities across America. More than ever, we hear horror stories that make CIOs at every school cringe—prestigious schools in the news for failing to prepare for the possibility of user information being stolen or lost.

One of the most recent examples is the University of California at Berkeley, where restricted electronic databases for UC Berkeley’s University Health Services were breached last year by hackers based overseas. In a laudable effort, UC Berkeley officials were quick to address the issue in a public and forthright manner with those affected by the data breach, and promptly took steps to put even more protections in place to try to prevent such a breach from happening again.

Still, at some point university CIOs have to ask themselves, “What else do I have to do to win this security marathon?” University ICT security professionals are in a bad spot. Whereas most companies have legal authority to access all user files and devices on their networks, universities do not. A university setting comprises one of the most dynamic ICT user populations out there. Teachers, students, and researchers access resources through computer labs and other institutional resources. They also bring personal computers on campus and plug in to the network.

Yet, unless the school’s security policies mention it, none of these systems and the data they contain are owned by the school itself.

Not Enough “Running” Hours

I recently spoke with a university CSO who had spent 20 to 30 hours per week for the last year just trying to develop processes and keep up with required policy work to comply with new regulations. With the strain on budgets and the size of ICT departments for most schools, this approach is just not tenable over the long term.

The problem is that compliance takes time, and for many there just aren’t enough hours in a day to keep up. That’s because they need to rethink the way they look at security—it goes beyond just product implementations. Like any good quality initiative, it begins with policies, process, and training. But it also must include enforcement; otherwise, the security policies aren’t worth the bytes they consume.

Why is this important? The motivator for campus data and system security is clear: It’s expected. Campus users expect security, and it’s a school’s responsibility to ensure it. The law also expects it. But in the end, any invasion of personal information reflects poorly on the reputation of everyone involved. If security weren’t an expectation, credit card companies and the government wouldn’t threaten imprisonment and massive fines to drive home the seriousness of the issue.

The security challenges are exacerbated by recent changes in regulations like PCI, HIPAA, and FERPA, and how those standards affect people whose identities and personal records are stored in university ICT systems. Today, there are several major
laws already on the books that protect information in university networks:

- The Gramm-Leach-Bliley Act (GLBA) protects personal financial information including the amount of assets, positions held in stocks or funds, outstanding debts, and purchases. While the Federal Trade Commission views universities as financial institutions, it ruled that universities that comply with FERPA are by nature in compliance with GLBA. This does not exempt universities from safeguarding regulations, though. Universities must adopt information security measures to comply with the GLBA Safeguarding Provisions.

- The Payment Card Industry (PCI) Data Security Standard is a guideline from credit card companies to help organizations that process card payments prevent credit card fraud and other security vulnerabilities or threats. Failure to comply risks losing the ability to make transactions and being audited or fined by the PCI Security Standards Council.

- The Health Insurance Portability and Accountability Act (HIPAA) outlines use and disclosure of protected health information (PHI). PHI is any information about health status, provisions for healthcare, or payment linked to an individual. In higher education settings, entities covered by HIPAA regulations may include university health services, hospitals, clinics, faculty practice plans, health plans, and potentially any department conducting research involving human subjects.

- The Family Educational Rights and Privacy Act of 1974 (FERPA) is a federal law that protects the privacy of student information and educational records, including foreign students’ visas. All schools receiving funds through the Department of Education must comply.

But none of these laws have any teeth if the university doesn’t create a strong, effective plan to safeguard users. In a recent ECAR IT study, 10 percent of the 435 institutions surveyed said they didn’t have any policy at all, while 37 percent had policies that were still in the implementation stage. That’s not going to get it done.

Most university policies are a combination of a confidentiality agreement and the school’s security policy. Policies should go beyond that to include security measures and procedures as well as an end-user agreement stating the individual’s agreement to comply with stated laws.

The breadth of coverage in each policy depends on the institution, but formal policies should include most of the following:

1. Appropriate use of institutional assets
2. System access control
3. Authority to terminate Internet access
4. Data security
5. Network security
6. Enforcement of institutional policies
7. Desktop security
8. Physical security of assets, residence halls, remote devices, and application development

Clearing the Hurdles

In my experience, it works best to take a nontechnical approach in writing the policy.
considering that most users on campus are unfamiliar with technical jargon and acronyms. Formatting a clear plan establishes user guidelines while enabling universities to remove unnecessary components of their security policies. A successful ICT security policy can be measured by how well various departments and university members are engaged in its development.

University ICT departments also need a plan to communicate clearly, broadly, frequently, and visibly with users, and to train them on the policies. Too often information policies are published and nobody knows about them.

Also, it is critical that policies be monitored and enforced. Some ICT organizations don’t see a significant decline in the number of incidents in their systems until they implement monitoring technology or procedures and widely publish discovered incidents. This is something UC Berkeley understood when it publicized the data breach so quickly after discovery, once the authorities had been notified.

Additionally, it is important to review processes from a security standpoint. It is surprising in this day and age how often users are asked to supply Social Security numbers in comment forms that don’t use SSL security. Changing processes that collect sensitive information is critical to successful policy implementation.

It may seem obvious, but universities should also ensure that all confidential information is obfuscated. It’s easy to be lax in maintaining credit card information, and users generally aren’t aware of the risks they take when entrusting their personal information to schools and corporations. Universities need to be clear that certain fields will always be in another format when reviewed (i.e., xxxx-xxxx-xxxx-5760).

Closing the Door on the Walk-Outs

Many university ICT departments wrestle with what data to encrypt. As a rule, start by encrypting any data that can easily “walk out” of your facility, such as laptops, desktops, tape drives, and removable media. It’s a smart idea to encrypt databases containing sensitive information, but unfortunately this is a decision universities end up making based on economics versus risks in too many cases.

Universities should also be using vendors that offer regulation-compliant solutions. They will need to appoint compliance project managers and create a plan. Regulations such as HIPAA and PCI add challenges to following requirements. PCI is often addressed by segmenting data and access with something as simple as a firewall. The PCI scope should be tightly managed, in case future compliance gaps require remediation.

Before hiring a licensed provider, a university should research and prepare for specific legal requirements when conducting internal audits. VeriSign recently released a report that analyzed the highest percentage of assessments that failed PCI audits. Top requirements that organizations failed to meet were protecting stored data, regularly testing security systems and processes, and assigning unique IDs to each person with computer access. Over 70 percent of all assessments failed in these categories. Paying close attention to weaknesses provides a solid framework to address issues before and after an audit.

Another common concern is whether a university needs penetration or vulnerability testing, or both. Most enterprise organizations just perform vulnerability (risk) testing. But a better approach may be penetration testing, which involves active exploitation of security vulnerabilities that could crash or disrupt a university’s ICT system.

Train for the Long Run

While all of this may sound intimidating, universities that include all stakeholders during implementation of a new or revised security policy have a higher degree of success. Ideally, the president, dean, board of trustees, internal and external auditors, and a campus task force with members drawn from key departments should be involved as the policy is developed. Execution of these policies should be shared with both administrators and end users.

Training and appropriate documentation should be set up with an internal audit conducted after implementation. Universities should work with their communications departments to maximize publicity about the new policies, either through on-campus advertising, social media channels or school website or newspaper. Messaging should explain that security changes help users, not just the school.

Juggling to keep a university system open and accessible while maintaining a secure network takes discipline. For instance, implementing a new plan may be delayed by other issues within a security policy. Universities shouldn’t hesitate to make ongoing revisions as long as changes are shared with users. Above all, this security marathon demands the focus of an elite athlete who understands that the race is not a sprint, but a journey.

Dave Durbin is the business development partner and a co-founder of Laurus Technologies. He can be reached at ddu@laurustech.com.
Security Snapshots of 3 Campuses

Miami University: Solid Security

At Miami University of Ohio, director of network engineering and telecommunications Chris Bernard says there is solid physical security, thanks to "a variety of measures based on the needs of what is being secured. We employ a range of proactive and detective-level controls, including monitored and unmonitored alarm systems, access control, motion-activated and continuous-monitoring video, and secured but unmarked rooms.

"The falling cost of Ethernet-connected video cameras led us to implement these in many of our critical areas," Bernard explains. "While these devices are not continuously recording, they are activated based on motion or contact, allowing us to track entry into secure areas."

In general, Bernard says, improvements at Miami have been made in the form of monitored alarm systems, of which the video monitoring is a part, with an eye to the school’s PCI compliance initiatives.

For instance, he notes, "we have implemented a control system that allows the wireless network to act as a single entity instead of thousands of individual access points. This allows us to detect rogue access points in the network down to a defined space, and if necessary, take the offending device offline."

Miami has not seen a major physical security incident, Bernard says, adding, "Most incidents we have experienced over the last few years have been situations where authorized personnel have mistakenly unplugged a device or bumped a cord, impacting service. In these instances we have used our resources to identify who or what caused the outage."

Notre Dame: Tight in the Core

At Notre Dame, physical security is tight for the network core, the distribution layer, the fiber in the tunnels, and the main MDFs, according to Jay Steed, director, Info security and privacy.

"The closets themselves are keyed to a unique physical key that is only accessible to our network engineers. However, on our main data center and our main network room, we have a two-factor biometric system," Steed explains.

Ongoing physical security improvements at Notre Dame also include a recabling program that covers three or four buildings annually. When a building gets recabled, if there is a shared closet, the network equipment is either separated physically or moved to a more secure location in the same building.

The university also has invested significantly to develop and maintain what Steed describes as a "fully compliant PCI cloud," involving numerous physical and network access restrictions where every network device and/or application processing credit cards must be placed.

Aside from physical security, Notre Dame has taken numerous steps to protect the network equipment itself. "What we have done is move our entire network management layer to a private network accessible only by VPN and two-factor authentication via secure key fob," Steed explains. "We have put Tripwire on every network device so we can tell if it has been altered or not. We also have intrusion detection and prevention systems on the network."

One notable security step is a border firewall policy that defaults to a closed state.

“Only about 15 specific ports are open to unsolicited inbound traffic,” Steed says. “We were one of the earliest big research schools to adopt a default closed policy. That required a good bit of cajoling of the research community to assure the research faculty that this policy wouldn’t hamper or otherwise interfere with their research.”

Texas A&M: Hardening the Net

“Physical security has had significant attention over the last decade,” says Dr. Walt Magnussen, Telecommunications Director at Texas A&M University, and he attributes that to a heightened awareness of physical threats triggered by the 9-11 terrorist attacks.

At Texas A&M, an initiative was launched to harden the network, starting with the core and working outward. Today, he says, the core is in good shape and aggregation points are solid; but in the IDFs and MDFs, the access portion of the network, improvements are ongoing.

“There is a lot of attention here to cybersecurity issues, but that’s understandable,” he explains. “The threat there doesn’t require physical proximity. But when it comes to our physical security, we have installed card access units at our aggregation points, so everyone is authenticated and there is logging. We have a Netbox security system, with cameras in all closets, along with temperature and environmental monitoring.”

Magnussen noted that redundant air conditioning and power is part of the Texas A&M hardening effort, pointing out that “this is a security consideration, since one of the easiest ways to shut down infrastructure is to disrupt the environment.”
Advertisers’ Index

By advertising in the ACUTA Journal, these companies are not only promoting products and services relevant to communications technology in higher education, they are also supporting our association. As you have opportunity, we encourage you to mention to these companies that you saw their ad in our journal and that you appreciate their support of ACUTA.

* Indicates ACUTA Corporate Affiliate

1Call, A Division of AMTELCO
Mike Friedel (800/225-6055)
4800 Curtin Dr., McFarland, WI 53558
info@1call.com
www.1call.com

Apogee
Nathanael Nealeigh (512/478-8858)
715 W. 23rd St., Ste. M, Austin, TX 78705
rnealeigh@apogee.net
www.apogee.net

AVST
Doug Juntwait (949/699-2300)
27042 Towne Centre Dr., Ste. 200, Foothill Ranch, CA 92610
sales@avst.com
www.avst.com

Chloride
Jeff Nasticky (847/816-6000)
27944 N. Bradley Rd., Libertyville, IL 60048
usa.info@chloridepower.com
www.chloridepower.com/us

Ciena
Jim Archuleta (410/829-4870)
1201 Winterson Rd., Linthicum, MD 21091
jarchule@ciena.com
www.ciena.com

Cisco
John Tuohy (408/525-7370)
3750 Zander Rd., San Jose, CA 95134
jtuohy@cisco.com
www.cisco.com

Dux PR
Kevin Tansillo (903/865-1078)
P.O. Box 1329, Canton, TX 75103
kevin@duxpr.com
www.duxpr.com

For details about advertising in the ACUTA Journal, contact
Amy Burton, Manager, Membership Marketing and Corporate Relations
Phone: 859/278-3338 x240 • e-mail: aburton@acuta.org
www.acuta.org
Kossuth: We maintain the same support services delivery that we have had in terms of a walk-up help desk, desk-side coaching, and education. The variety of devices we have been asked to support in some manner has increased as more options are available to students. Our support policies now often address the intersection of the technology with our enterprise systems. For instance, in terms of supporting smartphones we rely on the vendors to support the phones while we support the intersection of the smartphones and our e-mail system.

We attempt to provide more choice. For instance, we have a required laptop program. Based on student feedback on the usage of the Linux partition, we stopped providing a Linux image on the laptops and provided an Ubuntu distribution that students could access and elect to use based on their course or personal requirements.

Providing more choice and supporting the intersection of technologies requires flexible staff with the desire to stay on top of the emerging technologies and their support implications. More choice often equates to a longer service period for some help-desk tickets as well, so managing customer expectations is critical.

ACUTA: Since higher education seems to be perpetually in challenging budget times, what is your most important financial issue? How are you addressing it on your campus?

Kossuth: One of the challenges with central IT providing the vast majority of support for a higher education institution is that the costs of providing support are often not visible to other community members since the costs are not reflected in their budgets (especially when chargeback mechanisms are not in place). Creating an understanding of the costs of services and their connection to articulated priorities is an important piece of managing customer relationships.

A number of strategies have worked for us, including: sharing a spreadsheet of software usage and costs with the faculty committee and having the committee work with the faculty to narrow down the number of supported packages; putting up signs on printers (we do not charge for printing) detailing the costs of black-and-white and color copies; sharing a spreadsheet of the number of pages printed in various areas of the college; having departmental budgets support the difference in costs between the standard computer equipment issued and the equipment requested (and approved) by the various departmental entities; and creating a student/IT working group and working together to communicate projects, concerns, and brainstormed solutions.

ACUTA: Aside from funding, what issue are you, as the CIO, currently spending most of your time addressing?

Kossuth: Business intelligence and how to make our ERP system be flexible enough to provide us with critical information to meet the needs of an evolving institution and strategic plans.

ACUTA: What is the impact of this issue for your campus? What is your strategy for addressing this issue?

Kossuth: As the college evolves, the issue of metrics and reporting has become even more critical, and we need to enable community members to have data on demand in order to make informed decisions for the institution. We recently moved to Cognos 8.1, held a generic training for the community, and are moving office by office to implement the new reporting tool for critical reports as well as to distribute the reports (in icon form) to the appropriate community members. We have contracted with outside support to assist with this project over the summer.

ACUTA: Given that a key function of the CIO's responsibility is preparing the campus to support future technologies, what technology changes do you see for your campus as you look forward five to seven years?

Kossuth: As we look to the future, understanding how we will utilize cloud services (private, public, and other) in ways that provide us the privacy and security our data require will be critical to meeting the ever increasing need for "more and faster," especially in the areas of storage, research, and databases. That understanding is an important part of our strategy. We are already taking advantage of the virtualization era and will continue to do so to potentially reduce costs and to improve agility. Continuing to look at the technology use of our community members, we will be informed to make decisions on the technologies that should be provided by the college versus those technologies that can reasonably be expected to be provided by the community member. Mobility will play an increasing role in delivering our content to the community and to the wider world. Understanding the various support models for mobility and adapting our community to those models will be a challenge (including open source applications and mobile development which is already occurring on campus).

Over the next five to seven years, we will be replacing our network infrastructure hardware (already converged); partnering with additional outsourced assistance; and increasing our collaboration with academic partners. All of these will require us to find economical and effective ways to deliver on the increased demand and complexity of services in ways that enhance the experience of our community members and lower the barriers to technology adoption.

ACUTA: How are you readying the campus for these changes?

Kossuth: We will be working on development plans that address the different skill sets that are needed to manage the partnerships and outsourced assistance as well as the skill sets required to focus on integration and intersection of a myriad of tiered services. We are already working on developing relationships with the new vendor landscape for network services and will continue to do so in order to have everyone on the same page prior to our issuing an RFP. Finally, we have started conversations on these topics with the community so that we start to increase awareness of the changing landscape and allow the community to generate ideas as to what we need to be ready for and how. Regardless of the what and how, we can be guaranteed an increased demand for flexibility, services, and communication.

Thanks to Joanne Kossuth for taking the time to answer our questions. You may reach her at joanne.kossuth@olin.edu.

ACUTA Journal of Information Communications Technology in Higher Education Summer 2010
Q & A with the CIO

ACUTA: Much of the technology we now support in higher education is driven by consumer electronics. What decisions about your technology infrastructure have been affected by this and how?

Kossuth: In the past, higher education has often been persuaded of the importance of using "professional" grade equipment. This equipment was purported to have a longer lifespan, perform better and more consistently, and require a skilled knowledge set to utilize it. Today, these purported benefits are more often seen as "hidden costs." In addition, the current "prosumer" equipment that is marketed to the end users is viewed as simpler to use, "good enough," and easily replaceable with a newer, cheaper, faster generation of tools.

In terms of technology infrastructure, our audio-visual equipment decisions are now based on the simpler, good-enough model, and we expect replacements to be made more quickly (and the replacements can be justified in that they are quite a bit less expensive than the initial required investments). Our videoconferencing capabilities are up for renewal, and we are again leaning toward the "good enough" tools in Skype and other available online products with the replacement of just one "formally setup" videoconference facility.

Our telephony infrastructure has been VoIP since the opening of the institution. We initially invested in desktop speaker phones for everyone. With the increase in cell phone usage and ubiquity, we are now revisiting desktop telephones on an as-needed basis.

Last year, as part of our budgeting strategy, we discussed whether or not to consider all employees as independent contractors and to that end, expect the employees to provide their own laptops and phones. This conversation would not have taken place five years ago, and I would expect these types of conversations to continue as our employee and student base become more attached to their own electronic productivity tools.

ACUTA: Freshmen at most institutions today are far more extensive users of technology than those of even five years ago. What is the most challenging technical aspect this presents for your campus?

Kossuth: Most students arrive on campus with a good understanding of how to socially network (Facebook), text, Google or bing (aka search), immerse themselves in video games of some type, share photos (FLICKR or Picaso), and share files with their friends. In general, the students are used to home broadband connections and the ability to increase the connections as needed. They are also used to having a lot of choice or the ability to personalize their technology environments. Students do not generally understand an enterprise network structure, permissions or privileges, and the sharing of resources or the restrictions imposed by legislative or regulatory bodies or institutional policy.

Finding a way to effectively communicate with students regarding the changes to their technical environments when they arrive at college is an increasing challenge. Communicating the etiquette of using the myriad tools in ways that won't compromise their identity or their future job prospects is also critical. As cloud services evolve, they may provide a method of allowing additional individual choice in services (may have cost impacts on the students) which will more closely align with the home experience students are accustomed to. If and when this happens, there will also be increased requirements for education about privacy, security, and identity. Ideally these issues will be easier to address as technology evolves and imbeds additional tools to cover these areas as opposed to requiring additional add-ons and deep skill sets to protect the students.

ACUTA: In what ways has this affected how you deliver support services?

continued on page 39
Custom Entertainment
Create the perfect lineup for your residents with a hand-selected mix of campus, local, national and international programming. You can also offer optional HD, DVR and expanded movie and sports packages at no additional cost to you.

High Speed Broadband
Guaranteed bandwidth for each student, so peak hours don’t mean slow connections, plus 24-hour support for network and third-party devices like Xbox, iPhone, Tivo and more.

Digital Phone (VoIP)
Converged Voice-over-IP phone system allows you to replace aging PBX networks and still provide dedicated emergency phones and an in-room phone option for students who choose to have one.

Wall-to-Wall Wireless & Video-via-IP
Complete high speed wireless coverage lets students surf wherever they roam, while multiple channels of live IP-based television allow students to watch TV in real time on their desktop or laptop computers.

24-Hour Support
for all their network devices!

ResNet by Apogee
The one-stop solution for your entire student network.
Why add costly new PoE switches to support high power end devices when you can upgrade using your existing Ethernet infrastructure?

The solution: low-cost PowerDsine® Hi-PoE™ Gigabit Midspans

**Easy Installation.** Simply connect HiPoE Midspans to your existing switches to supply up to 32 watts of power for 802.11n access points, pan-tilt-zoom security cameras, IP phones and more. At about $50 a port, you’ll save a bundle — and boost the return on investment from your existing network.

**More Reliable.** Partnered with PowerDsine Midspans, your mission critical switches operate cooler, more reliably handling what they were designed for—communicating data. They won’t require bigger, hotter supplies just to power your new 802.11n devices.

**Energy Efficient.** PowerDsine Midspans only deliver the power each device actually needs. Only when it’s needed. Our exclusive PowerView Pro™ network management feature enables re-booting, individual port on/off, timed shutdown of unused devices, and much more. All controlled remotely.

Discover for yourself how easy, reliable and affordable our HiPoE™ Gigabit Midspan upgrades can be at:

http://www.microsemi.com/Powerdsine.

More power. Less cost.