University of Nebraska - Lincoln
DigitalCommons@University of Nebraska - Lincoln

ACUTA Journal

ACUTA: Association for College and University Technology Advancement

Spring 2015

ACUTA Journal of Telecommunications in Higher Education

Follow this and additional works at: http://digitalcommons.unl.edu/acutajournal

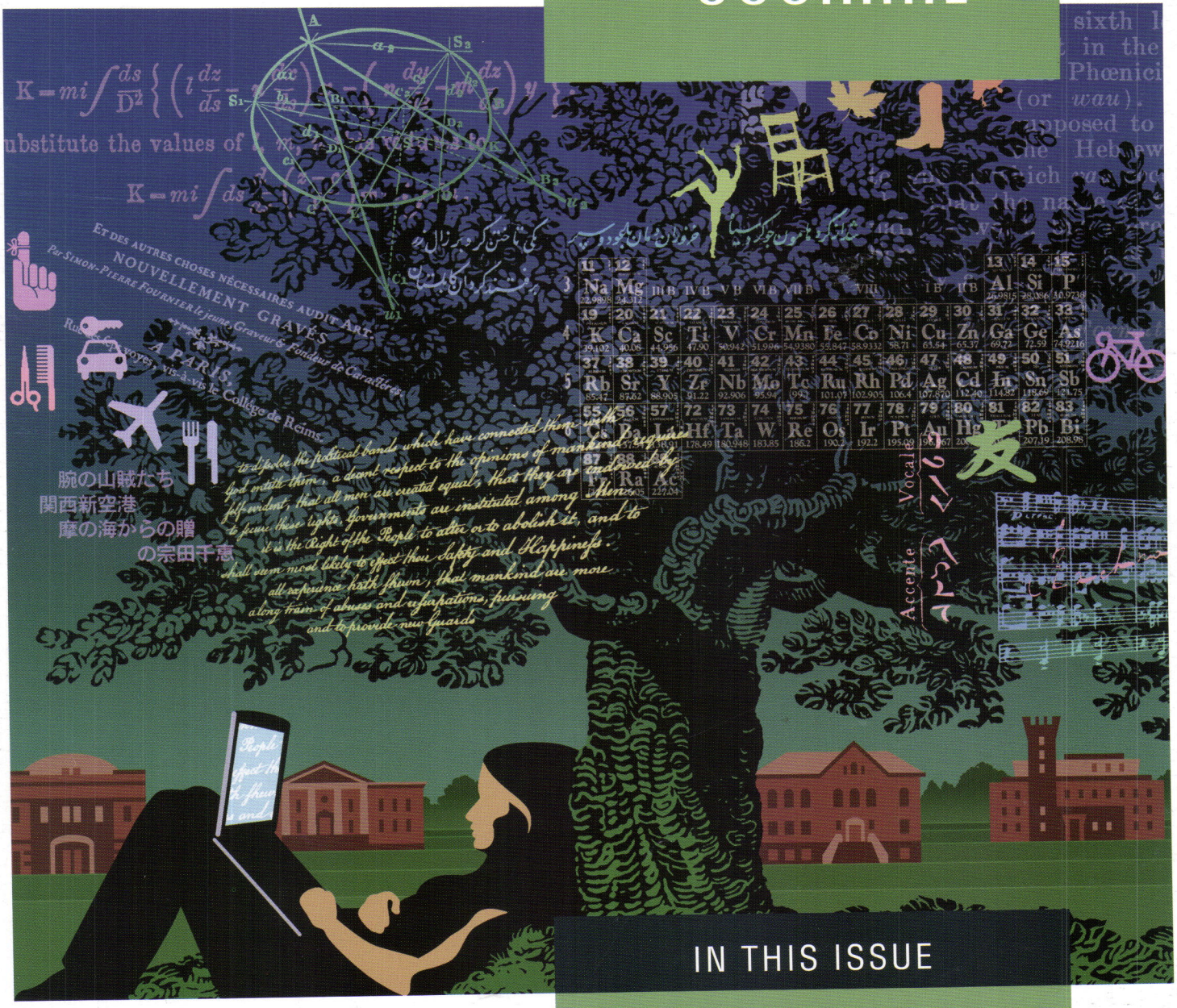
"ACUTA Journal of Telecommunications in Higher Education" (2015). *ACUTA Journal*. 79.
http://digitalcommons.unl.edu/acutajournal/79

This Article is brought to you for free and open access by the ACUTA: Association for College and University Technology Advancement at DigitalCommons@University of Nebraska - Lincoln. It has been accepted for inclusion in ACUTA Journal by an authorized administrator of DigitalCommons@University of Nebraska - Lincoln.

2015
Spring
Volume 19
Number 1

Association for College and University Technology Advancement

ACUTA JOURNAL



IN THIS ISSUE

The Bridge to Your Digital Future

Mobility

- Unified messaging
- Intelligent personal assistant – Atom
- Speech
- Location-based availability
- Single number reach
- Mobile client

Cloud

- Microsoft Office 365
- Google Gmail
- BroadSoft
- GENBAND
- RightFax Connect
- Mutare voicemail-to-text

Lync

- SIP integration
- Enables migration to Lync
- Enhances Lync with mission-critical voice apps
- First enterprise-class voicemail to resolve compliance issues

Internet of Things (IoT)

- UCConnect – extensibility to IoT and real-time event notification
- IoT is transforming the new digital business
- Connects data with communications to accelerate business decisions

Security

- Private messages
- Web client keeps messages out of email
- Mobile client keeps data off of your mobile device
- Mobile number protection
- TLS to encrypt SIP signaling
- Secure RTP (SRTP) to encrypt audio

Consolidation/ Optimization

- Scalability to 750 ports to support IT consolidation/ centralization initiatives
- Virtualization
- Interoperability
- Resiliency

Let AVST's unified communications solutions help bridge you to the world of digital business.

AVST

www.avst.com

Quotes of Note

Purdue continually faces challenges due to a growing number of personally owned wireless devices with unlicensed frequencies. Institutions need to ask the question, "What is the business need for greenspace wireless?" when cellular technologies can handle the required capacity.

Sue A. Lakin
Manager, Telecommunications
Purdue University
Lafayette, IN

The challenges in this business never end. Two of the big wireless challenges right now on campus are full accessibility vs. security and innovation vs. cost.

Mike Grunder
Senior Consultant, Vantage Technology Consulting Group
Concord, MA

The Year Ahead

Fall Seminar	October 25 – 28, 2015	Hyatt Regency Hotel Baltimore, Maryland
Winter Seminar	January 17 – 20, 2016	Hyatt Regency Hotel New Orleans, Louisiana
45th Annual Conference	April 24 – 27, 2016	Manchester Grand Hyatt Hotel San Diego, California

Core Purpose and Values

ACUTA's mission is to advance the capabilities of higher education communications and collaboration technology leaders.

ACUTA's core values are to:

- encourage and facilitate networking and sharing of resources
- exhibit respect for the expression of individual opinions and solutions
- fulfill a commitment to professional development and growth
- advocate the strategic value of communications and collaboration technologies in higher education
- encourage volunteerism and contributions by individual members

ACUTA

Association for College and University Technology Advancement

Spring 2015
Volume 19 Number 1

INSIDE THIS ISSUE

THE ACUTA JOURNAL

Publisher
ACUTA
152 W. Zandale Drive, Suite 200
Lexington, KY 40503-2486

859-278-3338 general office
859-278-3268 fax

Chief Executive Officer
Corinne M. Hoch, PMP

Editor-in-Chief
Pat Scott, Director, Communications
pscott@acuta.org

Contributing Editors
Curt Harler
James S. Cross, PhD

Advertising Sales
Amy Burton, Director, Strategic Relationships

Submissions Policy
The ACUTA Journal welcomes submissions of editorial material. We reserve the right to reject submissions or to edit for grammar, length, and clarity. Send all materials or letter of inquiry to Pat Scott, Editor-in-Chief. Author's guidelines are available on request or online at www.acuta.org.

The opinions expressed in this publication are those of the writers and are not necessarily the opinions of their institution or company. ACUTA, as an association, does not express an opinion or endorse products or services.

The ACUTA Journal is published four times per year by ACUTA, a nonprofit association for institutions of higher education, represented by communications technology managers and staff.

Contents of this issue of *The ACUTA Journal* are copyrighted: ©2015, ACUTA, Lexington, Kentucky.

ISSN 2151-3767

Postmaster, send all address changes to:

ACUTA
152 W. Zandale Drive, Suite 200
Lexington, KY 40503-2486
Postage paid at Lexington, Kentucky.

For more information: www.acuta.org
Membership and Subscriptions
Subscriptions are provided as a benefit of membership. The publication is available to non-members for $80 per year or $20 per issue. For information, contact Lori Dodson, Registration & Database Coordinator, 859/721-1658, or e-mail ldodson@acuta.org.

ACUTA 2014–2015 Board of Directors

President
Mark Reynolds, University of New Mexico
President-Elect
Michele Morrison, British Columbia Inst. of Tech.
Secretary/Treasurer
Riny Ledgerwood, San Diego State University
Immediate Past President
Ron Kovac, PhD, Ball State University
Directors-at-Large
Simeon Ananou, Salisbury University
Adrienne Esposito, Rutgers University
Sharon Moore, Smith College
Cathy O'Bryan, Indiana University
Christopher Waters, Elon University
ACUTA Chief Executive Officer
Corinne Hoch, PMP

Publications/Media Committee
Jeanne Jansenius, The University of the South, Chair
Abraham Arakelian, Vantage Tech Consulting Group
Tom Branam, Utah Valley University
Mona Brennan-Coles, Western University
Robin Burns, Principia College
Giselle Collins, Brit. Columbia Inst. of Technology
James S. Cross, PhD, Longwood Univ. (Retired)
Keith Fowlkes, Centre College
David Lutes, Marymount University
Toni McAllister, AVST
Andrew Nichols, Univ. of Illinois Urbana-Champaign
Doug West, University of Richmond

Ex Officio
Mark Reynolds, University of New Mexico
Corinne Hoch, PMP, ACUTA CEO
Janice Bundy, UCLA, Chair, Social Media Subcommittee
Amy Burton, ACUTA Dir., Strategic Relationships

Board Liaison
Cathy O'Bryan, Indiana University

Staff Liaison
Pat Scott, ACUTA Director, Communications

Editorial Review Board
Shad Ahmed, University of Rhode Island
Matthew K. Arthur, Washington University in St. Louis
James S. Cross, PhD, Longwood Univ. (Retired)
Alan Crosswell, Columbia University
Mike Grunder, Vantage Tech. Consulting Group
Paul Hardin, Brigham Young University
Joseph E. Harrington, Boston College
Ray Horak, The Context Corporation
Jeanne Jansenius, The University of the South
Walt Magnussen, PhD, Texas A&M University
Dave O'Neill, PhD, Community Colleges of Spokane
Cindy Phillips, Northern Illinois University
Carmine Piscopo, RCDD, Providence College
Patricia Todus, Northwestern University (Retired)
Pat Scott, ACUTA Director, Communications

COLUMNS

Advertiser Index

Correction
Our apologies to Nick Davis and the University of Wisconsin-Madison. In the winter issue of the *Journal*, we inadvertently printed UMW instead of UWM in the subtitle. We hope everyone read this fine article and never noticed our typo!

page 9

On one hand, historic living spaces can be an excellent selling point, especially at well-established institutions that have a distinguished history. On the other hand, students today are accustomed to certain modern amenities, and seamless WiFi is at the top of that list.

Kunal Hinduja

page 32

These fundamentally human concerns can be seen only as risks to be mitigated, or they can be viewed as invaluable opportunities to elevate and enrich an IT organization's role as a trusted partner.

J.D. Warnock

FEATURES

PRESIDENT'S MESSAGE

It's Been a Year Already?

by Mark Reynolds
University of New Mexico
ACUTA President, 2014–2015

Has it been a year already? This time last year I already had my ticket to Dallas and was ready to embark on the Grand Adventure of being president of ACUTA.

If you were at the conference last year, you may recall that my request, delivered in song with help from Adrienne Esposito, was that you "Stand by Me." And I'm happy to say that you have. It's been a great year.

During the past 12 months, we have focused on some activities and strategies that were designed to strengthen our association and further our professional careers. We looked at ways to develop leadership skills. We provided up-to-the-minute information on technology and higher-ed topics through webinars, seminars, and the conference. We changed some aspects of ACUTA's governance structure and invested in strategies to enhance our visibility and increase our membership numbers.

Beginning a year as a part of the governance structure of ACUTA at the Annual Conference is very motivational. If you are not a regular attendee—or if you have never come to the conference!—you may not realize what an inspiration it can be to interact with so many great people who not only understand what you do but actually enjoy talking about the job—because they do it too!

Our final session in Dallas was called "Conference Gold," and we left there with the top 10 "golden nuggets" that would be helpful to all of us. The top 10 list included the best Tweets of the event, such as "ITIL isn't teaching something new, but putting something you already know into best practices." That's sound advice, as are "IT departments should operate more like a startup than a Blue Chip" and "Information sharing is power: Be a collaborator, not a cowboy."

If you haven't already registered for this year's conference, do it today! Our Program/Content Committee chair and recently elected President-elect Arthur Brant will lead another great interactive session to close the event on Wednesday, and you won't want to miss it!

In April the ACUTA board began the steps necessary to complete a technology upgrade, upon the recommendation of the Technology Task Force. As we all know, that is a very complex task that requires a great deal of planning and energy. Thanks to everyone, especially ACUTA CEO Corinne Hoch and CTO Aaron Fuehrer, ACUTA now has an impressive new website that meets—or exceeds!—our needs in some very practical ways. Check it out at www.acuta.org if you haven't already experienced it.

In June we announced our new tagline: The Association for College and University Technology Advancement. This new wording better reflects the broad scope of communications as it has evolved over the past few decades.

This has been a busy year for ACUTA's Legislative and Regulatory Affairs Committee with issues such as net neutrality coming into the limelight again. ACUTA has continued to provide excellent information to members regarding what has happened in Washington relevant to higher-ed technology. Thanks to that committee and its chair, Eric Breese, for keeping us informed.

The Program/Content Committee, under the leadership of Arthur Brant and working with Michele West in the Lexington office, has done a fantastic job of providing high-quality programs to help us stay on top of the latest trends and big ideas this year. Sessions are available on the website for a good number of topics, such as "Meeting the Demands of Generation WiFi" from the Fall Seminar in Boston and "Wireless Do's and Don'ts" from the Winter Seminar in Anaheim. As an added bonus at the Fall Seminar, the Community College of Rhode Island invited attendees to its Security Awareness Day.

In September, ACUTA's DAS Task Force released the document it created to provide guidance to campus facilities folks when either constructing a new building or remodeling an existing building. The document, which defines what the task force felt was necessary in terms of building access, is available at www.acuta.org/das.

An Excellent ROI

As I draw near the end of my year as president, I encourage you to take a good look at your career and how your ACUTA membership can help you. ACUTA is one of the best investments you can make for your campus and your career. For a very reasonable fee, based on the size of your institution's enrollment, you get access to a wealth of information on the (new and improved!) website. If you need information about an emerging technology or the latest trend, go to the website and check out the *eNews* or the *Journal.* These publications are filled with information you can use.

If you need more than that, take advantage of the amazing ACUTA professional network by attending an event or simply posing your question to the listserv. If you aren't signed onto the listserv, you are missing out on a valuable tool that is literally at your fingertips.

ACUTA also publishes regular legislative and regulatory updates, provided by the "Leg/Reg" Committee and by distinguished legal advisors, J. G. Harrington from Cooley LLP in Washington, D.C., and Ken Salomon from Thompson Coburn LLP. You can get accurate opinions on all the latest legal issues with just a click.

You may be one of the many members who has taken advantage of the no-travel, low- or no-cost webinars ACUTA has added to the educational program. Technology has enabled us to stay current on some important issues without leaving the office, and that's another fine benefit of membership.

ACUTA was founded on the perceived need to interact with other professionals, and over the years, the conferences and seminars have been a valuable asset to many. Currently, ACUTA offers two dual-track seminars each year, one in January and one in October. These events focus tightly on two topics of relevance to IT/telecom, with knowledgeable presenters and an exhibit hall at both events. The Annual Conference brings hundreds of technology professionals together to examine a wide range of topics such as security, mobility, WiFi, networking, DAS, SIP, VoIP, and lots more. The biggest benefit of all for many, however, is the face-to-face networking that happens at every event. As I said earlier, it's not just inspiring but highly motivational.

As we all try to wear a growing number of hats on our campuses, we need to sharpen our skills and must never stop learning. I wish that everyone on the ACUTA roster could attend events. Our already fantastic network would be even greater! But we all have budget limitations and time constraints that often prevent us from travel and professional development.

However, there is much to gain just from being active in the organization. If you have never served on a committee, look at the list of committees that work behind the scenes to build a stronger ACUTA all the time. Find something that interests you and join the committee.

Consider the various award programs, such as the Institutional Excellence Award, and get your institution involved in the competition for this very prestigious award.

Run for an office on the board of directors. Your input will be valued no matter how large or small your school is. If you ask anyone who has served on the board, they will tell you the experience you gain is unequaled.

There are plenty of opportunities for growth. Just get involved.

What's on My Desk?

I have had a full year at the University of New Mexico as well. Like many of you, we are facing big issues on campus, including ubiquitous cellular coverage strategies, upgrading our voice and voicemail systems, upgrading the E911 system for future implementation of MS Lync, enhancing fiber infrastructure with copper reduction and removal projects, upgrading security, and on and on.

It has been a busy year at ACUTA, as well, and we expect to see results from our efforts in years to come. I have enjoyed my year as president, and I appreciate the support from all of you. I hope to see everyone at a future ACUTA event, and I will always be available if you just want to talk about the jobs that challenge us all. Thanks for standing by me.

Reach Mark at reynolds@unm.edu.

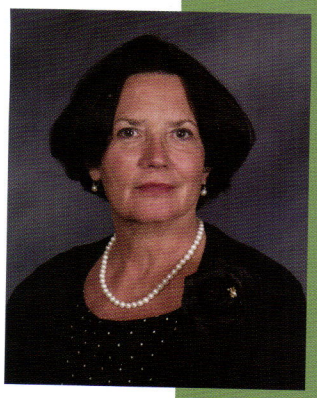
MiCTA
4805 Towne Centre
Suite 100
Saginaw, MI 48604
Toll Free: 888.964.2227
www.mictatech.org

MiCTA
Technology Solutions for Members Nationwide

- *Ready to use, competitively bid contracts*
- *18 Vendors currently under contract*
- *Competitive pricing*
- *Unique offerings exclusive to MiCTA Members*
- *Administrative cost savings*
- *Many new products and services available*

Watch for new RFP on Distributed Antenna Systems

Nationally, MiCTA represents members from all types of non-profit entities including: education, government, library, healthcare, charity, public sector and religious organizations. MiCTA produces and publishes collaborative RFPs generating agreements that are made available to all MiCTA members in good standing.



FROM THE CEO

Wireless, Net Neutrality, the FCC, and ACUTA: A High ROI

by Corinne M. Hoch, PMP
ACUTA CEO

Net neutrality has made headlines lately, and its impact on higher ed warrants a close look at the details. Let's go to ACUTA's experts for the latest information.

In this issue of the *Journal*, you may very well see yourself reflected in the articles on wireless security, 802.11ac, DASs, the Internet of Things, and BYOD… If you don't find something of interest in the ensuing pages, I'll be very surprised. ACUTA strives to provide a full complement of resources that will bring you solutions tailored to your needs. In the pages of the spring *Journal*, you will find articles relevant to the issues I just mentioned, plus another that is very important in our information repository—legislative and regulatory affairs.

To augment my column for this issue, I have turned to J.G. Harrington, attorney with Cooley LLP, for his comments on net neutrality issues that are relevant to higher ed. J.G. is a member of ACUTA's Legislative/Regulatory Affairs Committee, and his grasp of the impact of various legislation on higher ed is invaluable. I also would like to thank all of the members of our Legislative/Regulatory Affairs Committee for their commitment to providing you with the information you need in order to comply with ever-changing regulations.

With help from J.G. Harrington, Cooley LLP and Ken Salomon, Thompson Coburn LLP the committee, chaired by Eric Breese, monitors activities in Washington that impact higher education. This committee works diligently year round to represent the interests of ACUTA members. We have been closely following the actions taken by the FCC in the Wilson Booster case, and the FCC incorporated ACUTA comments in the final order. The following should be of special note for all of us:

Net Neutrality Position

ACUTA supports the concept of network neutrality and works with other higher-education associations to support legislation and/or regulations that seek to achieve this principle. We encourage you to follow our timely updates, such as the overview from Cooley LLP below, on net neutrality; blogs; the monthly leg/reg newsletter; and podcasts—and to reach out to us with any questions on higher ed–impacting leg/reg issues.

FCC Releases Network Neutrality Order

March 12, 2015. Today, the FCC released its 400-page order (including 80 pages of dissents from the two Republican commissioners) in the network neutrality proceeding. Despite speculation that some of the rules might not have been revealed in the FCC's previous public statements, the order contains few surprises. Highlights of the Order

- Scope of the rules: The rules apply to "broadband Internet access service," defined as any service, wired or wireless, that provides access to substantially all Internet end points, except for dial-up services. The rules apply to both licensed and unlicensed wireless services. The rules do not cover (a) "specialized services" that use Internet Protocol but do not provide access to the entire Internet, such as voice over IP service offered over cable facilities or medical monitoring devices; (b) enterprise, virtual private network, hosting, data storage, and Internet backbone services; or (c) "premises operators," such as coffee shops, bookstores, and colleges and universities that provide access to the Internet.
- **Blocking:** The rules prohibit blocking access to lawful content, applications, and services, or blocking use of devices that are not harmful to the network.
- **Throttling:** The rules prohibit impairing or degrading Internet traffic based on content, applications, or services, or an end user's installation of a device that does not harm the network.
- **Paid prioritization:** The rules prohibit paid prioritization, which is defined as using any technique to give some traffic an advantage over other traffic in return for any kind of payment or on behalf of an affiliated entity.
- **Transparency:** The FCC retained the existing rule requiring ISPs to disclose the terms and conditions under which they provide service, including prices and speeds. The new rules also require ISPs to disclose promotional rates, all data caps and allowances, and packet loss, as well as to provide specific notification of network practices that are likely to significantly affect consumers' use of the service. The additional requirements will not be applied to ISPs with 100,000 or fewer subscribers, at least initially.
- **General conduct rule:** Broadband Internet access providers cannot "unreasonably interfere with or unreasonably disadvantage" either end users or edge providers in the use of Internet service. This rule is in addition to the specific network neutrality requirements, and questions under the rule will be addressed on a case-by-case basis.
- **Interconnection:** The FCC concluded that what it calls "commercial arrange-

ments for the exchange of traffic with a broadband Internet access provider" are within the scope of the common carrier provisions of the Communications Act, and therefore subject to complaints that practices are unjust or unreasonable. It did not adopt any specific rules, but instead decided to "watch, learn, and act as required" in response to complaints.

- **Reasonable network management:** Most of the FCC's substantive requirements – but not the paid prioritization rule – will be subject to an exception for reasonable network management. Network management is reasonable only if it is "primarily used for and tailored to achieving a legitimate network management purpose." The FCC will consider technical characteristics of the provider's network in determining what is reasonable, but did not provide any guidance on how acceptable practices might differ between wired and wireless services. (This has suggested some concerns about how wireless providers might differentiate services as they move to 5G.)
- **Reclassification of broadband services:** The FCC determined that broadband Internet access should be treated as a telecommunications service subject to the common carrier requirements of the Communications Act. As described below, the order forbears from applying some of those requirements to broadband services.
- **Taxes and fees:** The FCC will not require broadband Internet access providers to contribute to the federal universal service fund today, but is considering whether to change the contribution rules in another proceeding, and could require contributions later. The FCC took similar action as to contributions to the fund that supports Telecommunications Relay Service. The FCC also concluded that the reclassification of broadband Internet access as a common carrier service would not affect the existing exemption from state and local taxes under the Internet Tax Freedom Act.
- **State regulation:** In addition to classifying broadband Internet access as a common carrier service, the FCC also reaffirmed that it is a jurisdictionally interstate service. Based on that determination, the FCC concluded that the service is not subject to state regulation. It also determined that its decision to forbear from certain types of regulation also precludes states from applying the same types of regulation.
- **Enforcement and interpretation:** The order creates new procedures for complaints about potential violations of the rules and for issuing advisory opinions on the permissibility of particular actions that ISPs might take. The rules permit formal and informal complaints to the FCC, and the FCC can take action to address specific complaints or take broader enforcement action to impose forfeitures or other remedies available to it under the Communications Act. While advisory opinions will not bind the FCC, they will immunize a party that receives one against enforcement actions unless the FCC specifically advises the party that the advisory opinion has been withdrawn.

Common Carrier Regulation

The reclassification of broadband Internet access as a common carrier service subjects that service to a much different regulatory regime than the one that applied to it as an information service. The order used the FCC's authority to forbear from applying certain regulations to craft a specific set of requirements for broadband Internet access that are related to, but distinct from the rules that apply to telephone service.

These are the most significant requirements that the FCC decided to apply to broadband Internet:

- **Limitations on Unjust and Unreasonable Practices:** The FCC will apply the core elements of common carrier regulation, which prohibit carriers from engaging in unjust and unreasonable practices and from unreasonably discriminating among customers.
- **Enforcement:** The FCC will apply the provisions of the Communications Act that permit parties to file complaints with the FCC about violations of the statute or the rules. Parties also will be allowed to file complaints in federal court, but the FCC urged courts to send cases to the FCC.
- **Customer privacy:** The customer privacy obligations of Section 222 of the Communications Act, which include a requirement to obtain customer consent before using information related to the customer for marketing purposes, will be applied to broadband Internet service. The FCC is not, however, applying the rules that implement Section 222 at this time, which leaves some question as to how broadband Internet access providers will ensure that they comply with the statutory requirement.
- **Accessibility:** The requirements to provide accessible services for people with disabilities will apply to broadband Internet service. Many of these requirements already apply through other provisions of the Communications Act.

These are the most significant requirements that the FCC decided not to apply to broadband Internet:

- **Pricing regulation:** The FCC will not apply any of its specific pricing rules to retail broadband Internet and, specifically, will not require providers to file and receive approval of tariffs listing their prices and other terms and conditions. It may review the reasonableness of rates, particularly for interconnection, on a case-by-case basis.
- **Contribution requirements:** As noted above, broadband Internet access providers will not be required to contribute to the federal universal service fund or to the Telecommunications Relay Service fund, at least initially.
- **Entry and exit requirements:** Broadband Internet access providers will not be required to obtain FCC approval to begin providing service, to stop providing service or to be bought or sold.

- **Telephone-specific interconnection and unbundling:** The interconnection and unbundling rules adopted following the Telecommunications Act of 1996 will not be applied to broadband Internet access. This includes requirements to permit resale of retail or wholesale services.
- **Truth in billing and slamming:** The FCC concluded that there is no need to apply these rules to broadband Internet access, particularly in light of the transparency rule.

The classification of broadband service as a common carrier service also permits providers to take advantage of some benefits of being a common carrier under the Communications Act. Most notably, the FCC determined that broadband providers will be eligible to use utility poles and conduits in the same way as telephone companies and that broadband providers will be eligible for universal service funding, provided that they meet other requirements in the Communications Act.

What Was Not Known Before

The FCC's previous public statements about the order described most of the significant decisions it contains. There were, as a result, only a few elements of the order that could be thought of as surprises. They included the following:

- **The paid prioritization rule covers affiliated entities:** The focus in discussions of this rule had been on third parties paying for preferential access to end users, but the rule also prohibits preferential access – even if no money changes hands – for affiliates of an ISP. This is similar to the non-discrimination rule the FCC adopted in 2010.
- **Waivers of the paid priority rule:** The order creates a process for waivers of the paid priority rule if an ISP can demonstrate that a waiver is in the public interest. The standards for waivers are strict; in fact, the order notes that waivers for telemedicine likely would not be granted because it could be offered as a specialized service.
- **Ability to rely on advisory opinions:** Some of the discussion during the FCC's open meeting suggested that advisory opinions would be entirely non-binding. However, the actual rules give the party that requests the opinion protection against enforcement action unless the opinion is revoked and the FCC gives notice. This makes such opinions more useful, although still only in a limited way.
- **Customer notice of network practices that are likely to significantly affect consumers' use of the service:** This requirement was not mentioned at the open meeting, and depending on how it is applied, could require customer-specific notice in certain circumstances, or simply require notice that particular kinds of uses (e.g., gaming) may be affected by specific network management techniques.

Next Steps

As the FCC indicated at the open meeting, the order will not go into effect until 60 days after notice of the decision is published in the Federal Register. There is no specific time for Federal Register publication, but an order this long may take two weeks or more to appear. The changes in the transparency rule also must be reviewed by the federal Office of Management and Budget before they can go into effect, and that could take six months or more.

Appeals of the decision can be filed as soon as the order appears in the Federal Register, and likely will be filed immediately. Because the FCC is treating this decision as a response to the D.C. Circuit's decision on the 2010 rules, it is likely that the appeal will go to that court. Filing an appeal will not automatically stay the rules, so if the court does not grant a stay, the rules will be in effect while the appeal is being considered.

The rules also could be overridden if Congress passes and the President signs legislation creating a different network neutrality regime. Unless the legislation largely follows the framework of the FCC decision, it does not appear likely that the President would sign it. Congressional Republicans also could try to overturn the decision through a legislative veto or a rider on an appropriations bill, but those actions also would require Presidential approval.

Keeping you informed about important decisions such as we addressed above is one of the unique commitments that ACUTA is proud to make to our members. It makes your ROI very meaningful.

At the conference every year, we recognize people and institutions that have been part of ACUTA for 5, 10, 15, 20, or more years. People decide to rejoin because of the value ACUTA brings to them through (1) educational resources such as webinars, seminars, and the Annual Conference as well as the publications—the *Journal*, the *eNews*, and the legislative/regulatory newsletter; (2) the professional networking that happens not just at face-to-face events but also on the great listserv where you can ask how others are handling the challenges you face; and (3) the positive relationships we develop with our corporate affiliates, who are happy to be considered partners for our mutual benefit.

Representation in Washington on issues important to higher ed, BICSI, and continuing education credits, exclusive benchmarking research discounts, training discounts at the SIP School and the DAS bootcamp, and many more benefits create additional value to make that ROI very impressive.

For 44 years ACUTA has been providing everything you need to make your current career great and your next one possible. We built a bridge from telecommunications to information technology, expanding with the industry, and we continue to strive to support IT all.

Reach Corinne any time at choch@acuta.org.

•

Wireless Challenges on Campus

Providing access on historical campuses requires a lot of planning

by Kunal Hinduja

Today's college campuses are inundated with mobile device users. In the past five years, students' primary form of communication has shifted to smartphones, tablets, and now wearables. These devices, which process more and more data each semester, have taken over the way students interact with each other, their friends and family at home, and many of their professors who have set up virtual classrooms and downloadable lesson plans.

The call for more wireless accessibility is also coming from the students' parents, who are concerned about their children's safety. More than 70 percent of 911 calls are made from mobile phones, making it critical that calls to police, fire departments, and emergency medical services connect on the first try and do not drop.

Unfortunately, academia has been struggling to keep up with the surge in demand for data. Some colleges are offering WiFi based on older, passive distributed antenna systems (DASs) or small-cell networks. Aside from bureaucratic red tape and other financial issues that face most of the commercial real estate world, universities have their own unique challenges when it comes to offering wireless accessibility.

Aging Infrastructure

Most new sports stadiums are well suited for a DAS, but even modern venues need upgrades for a sophisticated network that can support a high volume of data. For instance, a 2,000-square-foot head-end room might be needed to store all of the DAS equipment in the only available space beneath the grandstands. This keeps the inner workings of the system out of sight and ensures that the setup does not disrupt the revenue-generating operations of the venue. The room containing the DAS equipment can be outfitted with a waterproof membrane that protects it and the valuable electronics inside from water that could leak down from the seating area. Rooms also need HVAC, fire suppression, and a security system.

Older structures like the ones at many historic universities were not built with radio frequency (RF) in mind, making it a challenge to install the required fiber, coax, and antennas. Besides the physical materials, the RF design itself can be a challenge, given that RF doesn't penetrate concrete, steel, and thick load-bearing areas of structures. Newer buildings are more accommodating to the physical portions of the installation, but the new LEED standards still pose a challenge in RF design.

To circumvent these obstacles, engineers and construction managers need to provide more cabling and a greater number of antennas, routers, and amplifiers, which add to the hard costs of the project. To maintain the flow of an RF signal, we work around obstacles frequently. However, in the case of a century-old football stadium that seats 100,000 fans, the obstacles might be the frame and mechanics of the entire structure.

There also needs to be space for a DAS head end (four to six racks of space for each carrier), and a control station, and room to connect the two, including the appropriate amount of power and cooling. Square footage is always a rare commodity when building DAS projects, and the amount of DAS and ancillary equipment that goes into a head end can be significant depending on the size of the DAS. If the location of the head end is too far from the minimum point of entry or main electrical system, costs can skyrocket and more challenges in the design come up given that more fiber and coax are required.

A challenge within antiquated athletic venues is that there are no existing pathways to run cables. These conduits often have to be constructed from scratch inside the venue without disrupting operations, and they ultimately need to connect to the ceiling structure for antenna placement. If no cable trays are available to run fiber optics, the following tactics (which were discussed at a 2014 ACUTA meeting of stakeholders) can be deployed:

- Install two 1-inch conduits from either the closest IDF or the nearest accessible cable tray to the inaccessible antenna locations.
- There should be no more than a total of 180 degrees of bend without a pull box. This could be two 90 degree, four

Older structures like the ones at many historic universities were not built with radio frequency in mind.

45-degree, or one 90-degree and two 45-degree bends.

- All bends should be sweeping electrical bends.
- The conduits should terminate into a flush-mount deep electrical box.
- Refer to the local AHJ and Articles 810 and 820 of *NFPA 70 National Electrical Code* for requirements regarding coaxial cable installation.

Each carrier has its own set of standards and preferences when it comes to DASs. It is up to universities and third-party engineering vendors to be well versed in these standards, as they will vary depending on the carrier and the universities' infrastructure. Suppliers must make it a priority to stay as up-to-date as possible on the evolving standards of the carriers and continuously give feedback to the carriers for further development of their procedures. This process allows for a smooth working relationship with the carrier and the university.

Yesterday's Buildings Meet Tomorrow's Technology

College residence halls have a similar demand for data transmissions, but the challenges can be even greater. Users are not positioned within the line of sight of an antenna, as is the case in an arena. Everyone is confined by RF-blocking walls in a complex structure.

The capacity and signal quality of a DAS is especially important in residence halls since students, who are heavy data users, spend much of their work time in their rooms. Newer buildings tend to have room for additional cabling and mounting locations for the antennas, but older buildings have the same challenges as other university structures.

Schools that have older dorms, which are not suitable for RF, often require invasive retrofitting for conduits to run fiber and coax. This can be a catch-22 for the university. On one hand, historic living spaces can be an excellent selling point, especially at well-established institutions that have a distinguished history. On the other hand, students today are accustomed to certain modern amenities, and seamless WiFi is at the top of that list. To balance these conflicting virtues, the burden is on universities to invest in telecommunication upgrades while maintaining the historic charm of their buildings.

Lecture halls present an interesting situation in that they are smaller than an arena and larger than a dorm room. Although many can be served by an omnidirectional antenna, the maze-like structure that surrounds it can be complex and may prove very difficult to negotiate. America's higher-education lecture halls are built into some of the oldest buildings in the nation, which contain classrooms of varying sizes. From a tiny study group space of a few tables to a lecture hall seating more than 1,000, these rooms require varying levels of data capacity, and some are simpler to connect than others.

One of the most challenging aspects of installing wireless communications into these aging structures is navigating their architectural integrity. To get cables in and out, engineers often have to drill through limestone that was quarried hundreds of years ago. In addition to historic preservation guidelines and regulations, which make coring and drilling an issue, asbestos removal and the cost of x-rays that need to be done prior to installation add to the cost.

Academics, athletics, and on-campus housing are the three basic settings for college life. But a fourth type of facility perhaps serves the most important function on campus—university medical centers.

Typically the most modernly outfitted structure, these buildings are becoming increasingly dependent on mobile data. Doctors and patients alike are reliant on the sharing of medical information through mobile and medical devices, streaming data, and cloud storage. The difficult part about installing wireless solutions in medical infrastructure is that the operation cannot be affected even in the slightest. It's not like moving a class down the hall for a week. A hospital needs to run 24 hours a day, seven days a week, and it needs to be fully connected at all times.

Historical Preservation

Many universities are owned by the state and as such are subject to separate—and sometimes obstructive—preservation laws. For instance, a state might not allow a university to drill through its 200-year-old student union even if the project will bring an increased amount of data to the students and faculty inside.

Such provisions can often make or break a DAS or small-cell installation project and rewrite the university's wireless future. It is important for university IT managers to be familiar with the preservation laws to avoid conflict, work around them, or even try to override them through legislative means. With each layer of government, there are new levels of preservation regulations for historical structures, so this is not an easy task. But from an academic and economic standpoint, it is well worth the investment.

Public Safety

One of the most crucial tests for a wireless network is how it holds up during an emergency. College venues located in regions that are vulnerable to earthquakes or blackouts require special attention and some unique enhancements.

Antennas can be mounted with a chain that tethers them to the ceiling. If an earthquake shakes one from the structure, it would remain in a position that keeps the network intact and people safe during the chaos of the natural disaster. It is a critical feature because more than 70 percent of all emergency calls are made within structures from mobile phones, and those calls have to reach the outside world in order to alert authorities if there is a medical problem, an accident, or even a fire or natural disaster. Also, the wireless network maintains the open

FINALLY, STUDENTS CAN EXPERIENCE TV MOBILE WITH CAMPUS CONNECT. Students choose a university based on academics, cost, and yes, robust on-campus amenities like a seamless, easy-to-use experience. With our Campus Connect feature, you can provide your students access to live, streaming IP TV around campus on their own portable devices.

- On-Campus Access
- Safeguard Your Campus
- Reduce Internet Congestion

Contact us to learn more.
Visit coxbusiness.com/highered
or call (866) 419-6026

COX Business®

Available only to commercial bulk video customers with residential campus environments. Services and features not available in all areas. All services are not available for public viewing and pricing may vary. Installation charges may apply. All programming and pricing are subject to change. Other restrictions may apply.

radio frequency communication between first responders—such as police, fire, or emergency medical technicians—who are deployed to help someone in need. Without a strong communications system, lives could be endangered if something were to go wrong during a game or concert.

Final Thoughts

Meeting the needs of today's technology-driven campus and the expectations of a generation of students raised in front of a monitor certainly presents challenges as we try to balance providing appropriate infrastructure and maintaining historical integrity. It isn't easy, but with the right resources and careful planning, it isn't impossible either.

Kunal Hinduja is president of ARQ, a mobile telecommunications services company that has installed DASs for a variety of projects. Contact him at khinduja@arqwireless.com or visit www.arqwireless.com.

Snapshot

And Then There's Mass Notification

by Samuel Shane

Advances in modern technology continue to improve how we interact with each other and the world around us. We continue to see the development of better ways to complete both individual and organizational tasks faster and more efficiently with new or upgraded technologies. As old concepts take new shape, archaic systems and products are replaced with more advanced versions. And, many new technologies that were originally designed for one application are beginning to cross over into new areas. Following suit, security technologies offer several new options and capabilities that go beyond the typical uses in traditional applications.

A mass notification system's primary objective is to disseminate one-way communication to individuals or groups of individuals in the event of an emergency. It provides the fastest way to deliver a message to the masses when a crisis situation arises. However, with advancements in software technology and successful systems integration, mass notification systems have taken on a much broader scope of functionality. In addition to having the ability to send an intelligible audio broadcast to an enabled security communication device, new mass notification technology is making it possible for organizations to establish two-way communication to improve both internal and external operational processes. Additionally, recent changes made to the NFPA 72 2010 make it possible for emergency communication systems to broadcast informational messages.

Three delivery models for a mass notification platform are available, including hosted software, on-premises, or a hybrid of the two. While all three models make it easy to send thousands of notifications through text messages, e-mails, landline phones, pagers, fax, and BlackBerry Messenger, the future looks especially bright for the cloud-based version that is available as software-as-a-service (SaaS). The hosted application is available off-site where users can gain instant access to send alerts from a mobile or Web app through real-time connectivity to the Internet. The hosted platform requires no hardware or software installation.

The new mass notification technology is empowering corporations, educational institutions, and government agencies with new ways to use their existing communication tools beyond typical security functions to boost efficiency and improve operational functions.

Robust Data Centers Monitor IT Systems, Alert Staff

At the IT level, notification of events affecting data security and network outages can be sent to appropriate staff members immediately before they cause downtime or delays. The integration of data monitoring software into mass notification platforms eliminates the need for a business's IT staff members to monitor processes and systems. In the event of an issue, the notification platform will automatically send IT an alert so the employee on duty can quickly fix the existing problem.

Within a business, automatic reminders can be set up in advance on behalf of the help desk team members to cut down on expiring passwords and reset issues among employees.

There are several ways notification technology is helping facilities departments within organizations function more efficiently. Many businesses are using notification platforms to keep everyone informed about inclement weather and possible natural disasters. The technology not only allows the message to be

delivered to thousands of employees at once, it also provides a way for them to respond with important information.

Mass Notification on Campus

Colleges and universities embraced mass notification technology early on as a way to send out emergency messages to students, staff, and visitors on campus. Emergency communication systems aren't just for emergencies anymore. Many colleges and universities rely on mass notification to streamline day-to-day communications. Mass notification platforms are being used on campuses to alert faculty members about a meeting update and inform students that a class venue has changed or remind them of approaching or shifting deadlines, special events, or a change in office hours.

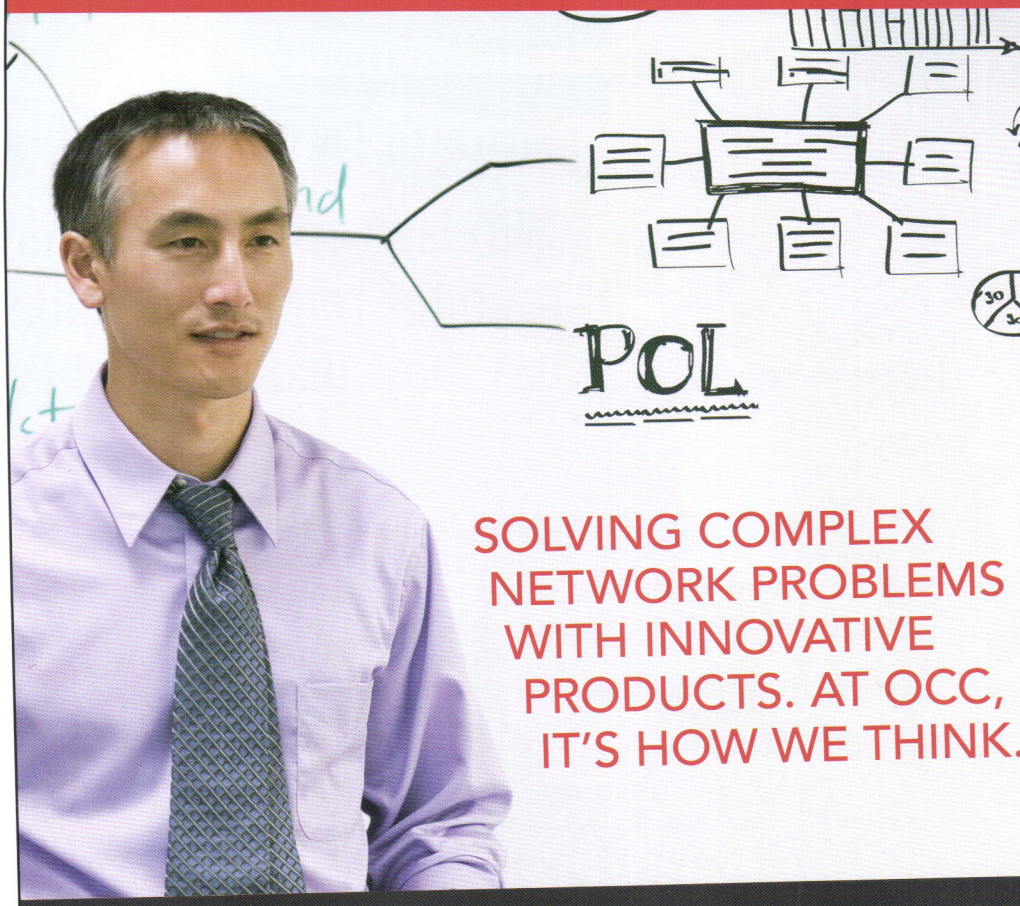
When storms hit, colleges are also using notification to inform students about canceled classes or building closures caused by unsafe conditions, flooded parking lots, and power outages.

Personal notification technology is also helping college officials reach students, staff, and visitors who are part of an updated database through text messages, e-mails, and social networks.

Conclusion

There are several more ways mass notification software has helped improve productivity and operational processes for businesses within a growing number of industries. We will continue to see the rise of mass notification technologies in new spaces, resulting in increased opportunities for integration beyond traditional security applications.

Thanks to Samuel Shane, chairman at Talk-A-Phone, for providing this information. Visit their website at www.talkaphone.com/ACB4 for additional information.



SOLVING COMPLEX NETWORK PROBLEMS WITH INNOVATIVE PRODUCTS. AT OCC, IT'S HOW WE THINK.

Consider OCC's Passive Optical LAN (POL). Available in ceiling, floor or wall mount options, OCC's POL has a smaller footprint, requires less cooling and fewer materials than traditional cabling networks, and lower installation costs and lifetime ownership savings.

The OCC POL. It's just another way the most reliable connectivity and cable manufacturer is the most innovative solutions provider in the communications industry.

TODAY'S OCC. STRONG. INNOVATIVE. SOLUTIONS.™

OCC®

800-622-7711 • Canada: 800-443-5262

occfiber.com

Time to Deploy Wireless Security Cameras?

Wireless connections enable campus police to monitor remote locations more effectively—but they also create challenges

by Paul Korzeniowski

With campus violence gaining more national attention than ever, security has become a hot topic on college campuses. In 2014, 15 incidents occurred at 14 different campuses from across the country (see Figure 1). In the attacks, 12 individuals were killed, and dozens were wounded.

Sexual assaults are also gaining more attention on campus. Mixing alcohol and hormones frequently leads to problems. In fact, the United States Department of Justice found that one in five women will be sexually attacked during their college years. As this area gains more attention, schools are taking steps to provide a safer environment for everyone.

Criminals seem to understand that their chances of getting caught increase with the availability of video evidence, and many are taking their nefarious activities elsewhere.

Wireless Systems to the Rescue?

Wireless security systems are one way to improve safety on campus, and interest in these systems is growing: Market research firm Research and Markets Inc., expects global CCTV revenue to rise at a compound annual growth rate of 12 percent from 2015 to 2020.

Schools understand that they need to take steps to protect students, staff, and college property. Traditionally, wireless security systems, dubbed closed-circuit TV (CCTV) solutions, have been expensive and difficult to operate. However, as costs go down and operating becomes more user-friendly, more schools are deploying these systems.

Deterring crime is obviously the main driver of adoption for these systems. Wireless cameras allow security teams to capture video as individuals and cars come and go. Police look for suspicious activity, such as cars circling past open spaces or a person lingering near an entryway. If suspect activity is identified, cameras allow officials to zoom in and take pictures of the individuals or car license plate numbers. Police can be dispatched to the location if needed.

"Universities want to have as much tangible data available as possible, so they can successfully prosecute and prevent crime," said David L. Perry, assistant vice president for safety who is also chief of police for Florida State University and president of the International Association of Campus Law Enforcement Officials.

Wireless security cameras help universities meet safety goals because they monitor local and remote sites seven days a week, 24 hours a day. Schools that have put in such systems report that crime has decreased—in some cases, quite dramatically. Criminals seem to understand that their chances of getting caught increase with the availability of video evidence, and many are deciding it's just not worth the risk.

In 2009, California State University Long Beach installed approximately 60 cameras—about two-thirds of which are wireless connections—across campus. "The number of crimes in the areas where we put the cameras dropped significantly—more than we expected," stated Pascal. The system helped campus police identify and arrest suspects; solve several break-ins and auto theft cases; and deter crime.

Benefits of Wireless

Wireless solutions have plenty of attractive features, starting with convenience. In many cases, parking lots, maintenance buildings, and dormitories sit in remote areas that are difficult to patrol. For instance, the University of Texas at San Antonio (UTSA) has a 600-space parking lot that is not close to a wired connection.

"The wireless system was the most effective way to get data from such a far-away area without the cost associated with a wired system," said Daniel Pena, UTSA assistant police chief. Cabling costs $.50 to $1.00 per foot, so the further away the location, the higher the cost. A wireless connection costs a few hundred dollars.

Wireless systems are less intrusive. Colleges do not have to dig up paths and clear areas as they would to lay wired connections. "To put in a wired connection, we would have been trenching all over the place, which is horribly disruptive," said Greg Pascal, communications and IS manager for the California State

University Long Beach Police Department. Schools sometimes lack the manpower and expertise needed to lay the cabling across campus and need to hand the work to outside contractors.

The cameras also have special features because they need to work in various types of lighting. During the day, plenty of natural light is available. At night, the systems must work in the darkness. When a scene contains bright, shaded, and intensely lighted areas all together, image quality can suffer.

Suppliers have developed various imaging technologies that help address the lighting disparity. For instance, security vendor Pelco, Inc., created SureVision, a system designed to significantly improve the viewer's ability to identify details in low or bright light. SureVision combines wide dynamic range, low-light, and anti-bloom capabilities, automatically adjusting to highly varied lighting conditions. So the quality is good even for a low-pixel camera.

A pan-tilt-zoom (PTZ) function enables remote operators to move the camera to different viewing angles. For instance, they may want to zoom in on a person trying to open a locked door or get the license number of a suspicious car. Here again, the range of options differs depending on the camera model.

A video management system helps law enforcement collect and manage the images. A school collects a lot of video, but how can it be used to improve security? Sitting and watching hours of tape can be time consuming. Vendors have addressed this concern by adding analytics capabilities to their systems to speed up viewing of the tapes. Also, in some cases, the security system automatically detects the presence of people and vehicles and notifies security personnel of a potential problem, so proactive steps can be taken.

Figure 1. Campus Shootings in 2014

Month	School	Event
January	Widener University	1 student shot and critically injured
January	Purdue University	1 student shot and killed
January	South Carolina State Univ.	1 student shot and killed
January	Los Angeles Valley College	1 student shot and killed
January	Tennessee State University	1 student shot in the leg
January	Eastern Florida State College	1 student shot
February	Univ. of Southern California	1 student shot
February	San Jose State University	1 knife-wielding student shot and killed by police
May	Paine College	1 student shot
May	Paine College	A second student shot one day later
May	Georgia Gwinnett College	1 student shot
May	Univ. of California Santa Barbara	A student shot 5 individuals (3 fatally), stabbed 3 fatally, and injured 4 with his car before committing suicide
May	Seattle Pacific University	3 students shot; 1 fatally
September	Indiana State University	1 student shot
November	Florida State University	3 students shot

The Budget, the Network, and Security Challenges

As good as they are, wireless systems do present college communication managers with challenges. The devices are expensive, costing twice as much as wired alternatives in some cases. Security applications are bandwidth hogs that often have a major impact on the quality of traffic traveling on campus networks. The solutions can be difficult to deploy and require ongoing care and maintenance in order to be effective.

Complicated wireless camera systems include many different components as they support a variety of functions. Video encoders are required at each end of the network connection, and cameras need to be purchased and installed. Logically, lower-priced systems typically deliver poorer resolution than higher-priced systems. Pixels are one area of differentiation. A pixel is a mark on a screen. The more pixels the system has, the better the image quality.

For the communications manager, the key element is the network connection. A wireless network link operates in a specific licensed band. Wireless computer network equipment typically uses radio signals in either a 2.4 GHz range or a 5 GHz range, and each has its own pluses and minuses. Cordless phones, automatic garage-door openers, and other home appliances run in the 2.4 GHz band, so interference becomes possible. The 5 GHz band is used only for wireless data communication. A 5 GHz network can carry more data than a 2.4 GHz network. The higher the frequency of a wireless signal, the shorter its range, so a 2.4 GHz network covers the larger range. Also, the higher frequency 5 GHz network signals do not penetrate solid objects nearly as well as do 2.4 GHz signals, limiting their reach inside buildings.

Whether or not to tie the security transmissions into the campus network is an important consideration. Video systems are bandwidth intensive. "We transmit 1 terabyte of information each day," noted Pascal at California State University Long Beach. That volume may interfere or overwhelm a campus network. If the transmissions are too great, then the video system may experience a blip or even crash, and the transmission appears

choppy, blurred, or blank. Such problems could render strong surveillance moot.

Security is another consideration. Some schools promote open access to network resources with few, if any, security checks in place to keep intruders out of the campus network. Consequently, outsiders may find it easy to gain access to the CCTV network. Since this system is used for law enforcement, the school may want to add security checks to the transmissions.

In some cases, a achool puts the CCTV system on a separate network. If the school's staff is not capable of installing the systems for any reason, third-party vendors are a viable alternative. When making such decisions, communication between the campus police and the communications department is needed to design the best system. "The communications manager and team were key to our understanding how to design the system; they were the network experts," noted Pascal.

Making It Work

Placement of the system is important. Law enforcement wants to get a clear picture of the activity taking place in an area. Meeting this desire can be difficult because natural and man-made impediments, such as trees, poles, and buildings, may block the viewing area. The placement often is dynamic. "We found that some locations did not offer as good a view later as they did initially," said Pascal at California State University Long Beach. Shrubs grow and campus configurations change, so the system has to adjust to those changes.

Depending on the location, other ancillary items may be needed. Cameras may be located on light poles and other structures placed around campus. The cameras need to be tamper proof, so they typically are housed in protective casing.

Finally, schools have to make it known where and what they are recording around campus. Signs must be posted and visible in any areas where surveillance occurs.

Vendors Jump into the Market

The growth of wireless security on campus has attracted a variety of vendors to this field, including ADT Security Services LLC; Axis Communication; Bosch Security Systems, Inc.; Flir Systems, Inc.; Hangzhou Hikvision Digital Technology Co.; Honeywell International, Inc.; Panasonic Systems Networks Co., Ltd.; Pelco, Inc.; Samsung Techwin; Schneider Electric; Sony Corp.; Toshiba Corp.; Tyco International, Ltd.; Vicon Industries, Inc.; and Zhejiang Dahua Technology Co., Ltd. Competition should bring prices down making the technology an option for more campuses.

Final Thoughts

Security is becoming an ever-more important consideration on many campuses. Consequently, universities have been searching for ways to improve their surveillance systems. Wireless systems offer them a way to more closely monitor suspicious activity; but deploying these systems is a complex task, one that requires plenty of informed planning as well as close cooperation between the communications department and the campus police.

Paul Korzeniowski is a freelance writer who specializes in communications issues and is based in Sudbury, Mass. He has been writing about these issues for more than two decades and can be reached at paulkorzen@aol.com.

ASPIRE TO LEAD

ACUTA 2015
Association for College and University Technology Advancement

ACUTA Annual Conference & Exhibition
Atlanta, Georgia — April 19-22, 2015

Leaders are not born, they are forged by experience, challenges and opportunities. Your time to lead is here as campus administrators increasingly look to you for strategies and recommendations that shape multi-million dollar investments. They look to you to solve problems when there is no manual to turn to. In fact, when you do your best work, few notice; things just – work.

From **April 19 – 22, 2015**, technology leaders will meet in **Atlanta for ACUTA's 44th Annual Conference and Exhibition**. Professionals just like you will share the latest information and their experiences, review the leading-edge technologies and services, and discuss the best ideas for confronting tomorrow's challenges. You will be writing the manuals for your own progress.

If you want to be part of shaping the future of campus technologies, if you want to meet and be inspired by your peers, if you have a vision for your campus that you want to share, then aspire to lead and come to ACUTA's Annual Conference.

DELIVER
ENGAGE
LEARN
ADVANCE

Five Steps to Simplify and Secure BYOD

How do you accommodate multiple devices without compromising security?

by Trent Fierro

Colleges and universities are at the forefront of bring-your-own-device (BYOD). For years, students have arrived on campus with their own devices—laptops, smartphones, e-readers, tablets, and gaming consoles—expecting to connect to the network. Faculty, too, are bringing personal devices into the classroom to enhance teaching and simplify their own lives.

Most institutions are eager to leverage BYOD to expand the learning environment from the classroom to anywhere, anytime. This presents IT with a significant set of challenges: How do you provide ubiquitous connectivity for the sheer number and variety of devices arriving on campus and ensure a reliable user experience without sacrificing security and control?

Wireless provides the means to make network access ubiquitous. But to accommodate secure mobility for BYOD, IT needs to accurately identify each user, provide appropriate privileges, and maintain connection records for troubleshooting and compliance needs.

Oftentimes these tasks are supported via a wireless controller, which also provides RF management, traffic forwarding, application controls, and other network services.

As the number of user devices and authentications increase, it's now becoming a best practice to offload the security features to a dedicated access platform.

According to industry research firms, including Gartner, IDC, and Forrester, features that are key to successful BYOD environments include unified access with a single platform for policy management, security, and enforcement, as well as services such as onboarding and guest access.

Let's look at five of the most common issues IT faces in higher education and consider some tips and best practices to help simplify and secure BYOD.

Workflow Automation

In the age of BYOD, IT can't directly manage user devices, and it's not realistic to manually configure access and security settings on every mobile device across the entire institution.

It's now necessary to streamline the configuration of security settings, SSIDs, and device registration. IT needs workflows to be automated and, to the degree possible, to leverage a self-service model. In particular, users need the ability to onboard and configure their own devices without IT involvement or help-desk assistance.

The best way to accomplish this is with Web-based portals. The portals enable students, faculty, staff, and other regular users to self-register their devices for network access and to configure them with proper security and authentication settings. In addition, IT can enable users to register devices such as projectors, printers, and Apple TVs by simply filling out an online form.

Likewise, a captive portal provides visitors with simple and secure guest network access, so alumni, potential students, visiting scholars, and other visitors can get onto the WiFi network without burdening the help desk. IT can also use the portal to personalize the guest experience, as well as to promote campus events, services, and amenities.

The MAC address of each connected device provides a means to create policies that allow or deny access. For example, students—and their devices—come and go, as do guests, so IT can set a timer to age-out these addresses. For instance, student addresses can be aged out at the end of the academic calendar, while guest access can be limited to 24 hours.

It's now necessary to streamline the configuration of security settings, SSIDs, and device registration.... In particular, users need the ability to onboard and configure their own devices without IT involvement or helpdesk assistance.

Workflow automation has numerous benefits for IT, and also improves the user experience by giving users control over provisioning and onboarding their own devices, when it's convenient for them.

Differentiated Access Policies

With BYOD, it's crucial to define access policies based on the user role—such as faculty, administration, staff, and students—as well as to define device roles. For example, IT needs the ability to identify campus-owned computers,

printers, and other devices from BYOD devices, and to control how each class of user and device is given access to network resources.

To illustrate, a student may be allowed to access the business school network using his laptop and smartphone, but not his gaming console. Likewise, IT needs the ability to set appropriate policies for guest access. Guest and campus traffic should remain separate even though they share common wireless infrastructure.

It helps to have a policy management system that includes AAA services and provides both role- and device-based enforcement. In granting access rights, a policy management system should leverage contextual data such as user roles, device types, location, day of week, and time of day, and continually confirm the identity of the user employing that device.

To authenticate users and authorize the use of resources, a policy management system must be able to leverage multiple identity stores, from internal databases to LDAP-compliant directories. Support for multiple identity stores enables IT to manage and enforce policies across multiple domains, such as autonomous departments, ensuring that policies are applied consistently across the institution.

Optimal Bandwidth

BYOD can also create bandwidth challenges on campuses that can undermine user confidence in the network. One challenge is that older, slower devices must coexist with newer, faster ones, and older devices can slow down everyone. To avoid this problem, the WiFi network needs to optimize the connection for each type of device.

Network congestion is another problem, particularly as students, teachers, and staff bring multiple WiFi-enabled devices onto campus. Since WiFi is a shared medium, IT needs a way to expedite education-related traffic in classrooms and lecture halls and to constrain personal traffic, such as students who want to use Hulu, YouTube, and Netflix just for entertainment.

To deliver the performance that students need in crowded academic environments like lecture halls and media-rich surroundings such as dormitories, IT needs to ensure that the campus has adequate and intelligent WiFi capacity.

WiFi coverage must extend pervasively to all parts of a campus, with uniformly good signal levels. If you currently have 802.11n WiFi, consider deploying 802.11ac gigabit WiFi in areas that serve the highest number of users. Then, over time, migrate fully to 802.11ac WiFi.

RF management techniques should be employed to maximize coverage and network capacity, while avoiding interference. The WiFi network should also have the capability to recognize delay-sensitive traffic, such as voice and video, even if they are encrypted or appear as Web traffic.

To differentiate traffic and control it appropriately, invest in next-generation mobility firewalls that perform deep packet inspection. Wireless-specific firewall controls provide granular application information that lets IT make informed decisions about allocating WiFi bandwidth for critical apps, as well as implement quality-of-service policies, such as prioritizing education-related application traffic.

IT can also use this information to control bandwidth-consuming peer-to-peer traffic from clients like BitTorrent that originate from WiFi-enabled devices.

Stay Connected While Roaming

Keeping users connected as they change location is also a crucial component when supporting BYOD. Authentication can be done on a daily, weekly, or per-semester basis, and the network designed to span the campus; but, in a poorly designed network, as students walk between buildings checking their class registration status or grades, they can potentially bring a wireless network to its knees due to re-authentications.

Providing uninterrupted roaming can be tricky, in part because smart devices go to sleep and wake up over and over throughout the day. When large numbers of devices wake up simultaneously across the campus (for example, as class periods end), the authentication infrastructure can get overwhelmed, causing connectivity problems and poor user experience.

Both the WiFi infrastructure and the authentication services have roles to play in roaming. At a minimum, there needs to be sufficient WiFi coverage to support roaming. In addition, the WiFi solution must optimize connections and keep them from dropping.

Some WiFi solutions include traffic optimization features that ensure a user device connects to the best access point. For example, a smartphone typically connects to the first access point it encounters and stays connected, even if the user roams far away. The WiFi solution should be smart enough to hand off that user to the nearest access point with the strongest signal.

IT also needs to provide authentication services that can follow users wherever they go and keep them connected as they change location. The authentication services need to scale to accommodate the increasing number of devices coming onto a campus.

Given these requirements, IT must determine when offloading authentication from the WiFi infrastructure to a dedicated authentication solution makes sense. Using a dedicated solution frees the WiFi infrastructure to optimize the RF environment without being bogged down handling authentication requests.

Visibility and Reporting

Understanding what connects to a network is also an important BYOD consideration. To address performance and compliance requirements, IT needs to know where devices are being used, how many per user, and which operating systems are supported.

For example, if a university is informed that an illegal movie download has been traced to an IP address on its campus, IT needs the ability to trace all the activity tied to that IP address.

To ensure proper management, planning, and reporting, IT needs per-session logs and a tool that monitors network connections, fingerprints devices, and provides visibility into each user and device. A policy management solution that provides robust monitoring will help administrators identify and resolve WiFi and authentication issues quickly.

For planning purposes, IT also needs trend analysis capabilities. For example, if an increasing number of network devices are seen in certain areas of the campus, such as dorms or the student union, you can schedule a WiFi upgrade or expansion in those areas first. Knowing which access points are starting to reach their capacity makes it easy to plan ahead and keep the network optimized and available.

Achieve Your BYOD Goals

Education leaders see BYOD as an opportunity to diversify and expand the teaching and learning environment and to increase student engagement with technology and technology-enabled learning. A robust WiFi solution lets you achieve the goal of anytime, anywhere network access while simplifying life for IT and improving the end-user experience.

Today's WiFi and policy management solutions are sophisticated and robust, enabling higher-ed institutions to fully—and securely—embrace BYOD. In addition, leading institutions are leveraging vendor ecosystem partnerships to extend the functionality of their WiFi solutions with additional services, such as single sign-on and firewalling, from third parties.

BYOD in higher ed is no longer something to just live with—it's something that needs to be managed. With the right solution, you can embrace BYOD, simplify operations, and ensure a solid user experience regardless of what a user brings to campus.

Trent Fierro is a product and solutions marketing manager at Aruba Networks with responsibility for developing and executing Aruba's ClearPass and BYOD strategy. He has more than 15 years of industry experience with field sales and senior product marketing management positions at SynOptics Communications, Cisco, Net Optics, and Avenda Systems.

Another Line of Defense

EduLok is a multifactor authentication that the developer says is far more secure than anything else on the market. The technology requires a token—either a physical passkey or the mobile app—to log in to secure networks and servers.

Even if a server is hacked, the technology prevents hackers from getting all the puzzle pieces they need. The technology encrypts user data and fragments and disperses it across 12 locations worldwide, where it is no longer accessible to identity thieves, thus producing an unparalleled level of security specifically for the education industry. Even EduLok (www.edulok.com) can't access it, and data do not remain on the passkey or phone. The idea is that data cannot be compromised if it does not exist.

With an EduLok passkey, students and staff can access private networks, Web portals, e-mail, and applications without the need for numerous, antiquated, and vulnerable username and password combinations. Instead of providing a username and password to gain access, the user connects a physical passkey token to the USB port or NFC reader or connects the mobile token via Bluetooth technology or WiFi. The passkey triggers EduLok's cloud technology, accessing the data. Neither the physical token nor the mobile solution contains any personal data.

The solution comes in two versions. The Standard Edition gives access to a mobile passkey security token for a small per-user monthly fee, and the Pro Edition includes the mobile passkey and a full set of physical passkeys, plus the ability to manage multiple tokens for an additional charge.

Where Wireless Rules

A view of two solid 802.11ac deployments

by Curt Harler
Contributing Editor

If college IT staffs had cheerleaders, the cry in every computer center would be, "Wireless Rules! Legacy Drools!"

Even without pompons and sis-boom-bah, both college administrators and network managers know that the number-one players on campus are on the WiFi team. And there will be a WiFi dynasty ruling campuses for quite a while to come. That gives campus technology managers a challenge both today and down the road. It is not enough to roll out some flavor of WiFi and call it a day.

University of San Diego

At the University of San Diego (USD) in California, the move to WiFi was not championed by the traditional drivers like network efficiencies or dollar savings.

If you are rolling out WiFi, go big or go home.

"Our students demand WiFi," says Douglas Burke, senior director of network infrastructure, systems, and services at USD. USD is a private university with more than 8,100 students and 875 academic staff. They want it everywhere, as Burke discussed at ACUTA's Winter Seminar in January.

Over the past several years, USD had been implementing an ad hoc mixture of wireless devices from 3Com, Foundry, AT&T, Apple, and, as Burke discovered to his chagrin, "whatever the students or faculty brought in from home."

In 2005, the college settled on Aruba as its wireless provider. "We began installing their APs (access points) in the residence halls, our Law School and School of Business," he says. USD's move to gigabit WiFi was kicked off with three pilot programs conducted in various locations on campus.

Going into 2015, USD is finishing up the first phase and preparing to enter the second phase of its wireless implementation.

USD's network is 10 gig between the core and data center. "Distribution networks are built with 12 Cisco Nexus 7000 (9-slot) chassis in highly available (HA) with redundancy," Burke says. "Our edge switches are going to be replaced with 3750x (802.3at) with 10 gig uplinks to the distros."

USD has cabled and terminated CAT6a all of their classrooms and offices. "Phase II will cable the residence halls and Phase III will be the purchase and installation of new switches and Wave 2 access points," Burke says. The new infrastructure at USD will support more than 15,000 unique devices daily, providing a truly mobile environment in classrooms, residence halls, academic offices, and meeting places as well as outdoor locations—even the university's tram stops.

As for Phase II, USD is being very strategic, anticipating Wave 2 technology. "We still want to keep moving ahead with cabling the residence halls with CAT 6a and upgrading the edge switches to the 3750x," he says.

"Timing was critical for us since 802.11ac was/is not ready for prime time and our cabling Phases I and II are strategic to give the WiFi industry time to catch up with the standards," Burke says. In particular, they are looking forward to Wave 2.

"We aren't planning on spending money on Wave 1 products just to throw them out in 12 months for Wave 2," Burke says.

West Chester University

The situation was a bit different at West Chester University (WCU) in Pennsylvania. With 16,000 students and 1,700 faculty and staff, WCU is the largest of the 14 universities in Pennsylvania's state higher-education system and the fourth-largest university in the Philadelphia area. According to *U.S. News & World Report*, WCU is one of the top regional universities in the north. West Chester also is one of only three Pennsylvania schools ranked in the top 100 Kiplinger "best buys" in American public higher education. In fall 2013 the university began offering its first doctorate, the doctorate of nursing practice. A blossoming reputation like that has to be backed by solid infrastructure.

"We had to select a platform that was scalable to meet future WiFi needs," says Adel Barimani, vice president for information services and chief information officer at West Chester.

The school faced a unique opportunity. In the course of designing five new state-of-the-art student living facilities, the IT department realized that a high-speed WiFi network could be used

for all network access as an alternative to the wired Ethernet access network to significantly reduce costs and at the same time provide access convenience for students using several mobile WiFi-enabled devices.

"Given this opportunity, we created an all-wireless environment using Aruba Networks wireless solutions to deliver high-performance WiFi to students," Barimani says. With the arrival of gigabit WiFi, WCU also deployed an all-wireless enterprise solution, starting the major deployment with the new residence halls. The solution leveraged the 802.11ac standard to deliver the coverage, capacity, and performance needed in many of the residence halls. The time frame was to accomplish this task by fall 2014 for the latest residence hall and some other traditional residence halls.

To ensure a successful rollout of the new 802.11ac wireless network, West Chester conducted a pilot within a three-story building to confirm that throughput was maximized and the new technology would meet the school's needs.

For the new residence hall, it was a matter of planning and cutting the cord and only deploying WiFi. The traditional residence halls had only wired access prior to this current WiFi deployment. Today at WCU, the newer residence halls are totally wireless, but the solution uses basic infrastructure deployment and the campus backbone for general connectivity, with fewer switches deployed.

Other Networks

If you are rolling out WiFi, go big or go home. One of the concerns many IT directors face is bandwidth competition from other devices.

USD went big. "We saturate the airspace," Burke says. That gives them the upper hand on the airwaves.

"We faced a significant IT challenge," Barimani says. "Our 5,000 students living on campus were bringing their own wireless routers and plugging them into the wired ports in our residence halls and student apartments." This was quite similar to the challenge at USD.

As the volume of these routers grew, the problems caused by interference—and the resulting calls to WCU's help desk—escalated. "Clearly, we had to figure out a better way to deliver the reliable, high-performing wireless access our students were demanding, while meeting the network security and cost-efficiency parameters that our IT department required," he says.

Barimani says they experience occasional interference from items such as microwaves in the dorm rooms. However, they were relieved to find that other general wireless devices have not had a major impact on the system.

"Similar to any major deployment of WiFi technology, the system will have its general issues as new operating systems

Introducing
CloudReseller
The Voice of Enterprise Cloud
A monthly report on cloud communications for the enterprise.
Visit us at www.cloudreseller.com and www.telecomreseller.com
TelecomReseller™
THE VOICE OF UNIFIED COMMUNICATIONS
NETWORKS • IP/IP-PBX • VOIP • SIP • SOFTWARE • SERVICE • MAINTENANCE

are installed on mobile devices or new devices come on the market before the latest patch deployments," Barimani acknowledges. However, he is confident that companies—including Aruba Networks—have been staying on top of releasing patches timely to avoid major problems.

"Technology, in general, is a moving target, and you have to continue to be vigilant about upgrades and maintenance," he says, noting that new WiFi mobile devices show up on the market and in the stores on a weekly basis.

"We have nearly 60,000 unique devices on our WiFi deployment regularly," Barimani says. "With the latest release of wearable technologies such as smart watches and other WiFi devices, this mobile device number on the WiFi network is only going to increase."

WCU definitely went big, too. The new infrastructure comprises more than 1,000 indoor and outdoor access points with Aruba ClientMatch technology, which intelligently pairs wireless devices with the best available AP to ensure the highest network performance and the best user experience. It does this by gathering performance information from mobile devices and using it to intelligently steer each device to the best AP based on signal strength, traffic load, and connection type.

"In my opinion deploying WiFi minimally is no longer an acceptable scenario," Barimani says.

Securing the Wireless

"IT security, in general, is always a major concern. It is no longer a matter of 'if' there will be a security breach, but 'when,'" says Barimani. "We all have to be prepared for that, and in the meantime we have to be vigilant in working with vendors to ensure that security protocols are up-to-date."

For specific WiFi security, West Chester selected Aruba's ClearPass Access Management System, with the Guest, OnGuard, Policy Manager, and QuickConnect modules. "This system provides us with solid security features. ClearPass combines context-based policy management with next-generation AAA (authentication, authorization, and accounting) services for secure connectivity," Barimani says.

"We use WPA 2 to encrypt the packets between the client and the AP," Burke says.

Staffing the Project

WCU currently has one full-time person assigned to WiFi. "We have one full-time WiFi specialist, and other team members in our networking department help out as needed," Barimani says.

"We are exploring the possibility of adding one more full-time employee in that area," Barimani says. "For client support we rely on WCU's help desk teams including our residential IT help desk group to support faculty and also students."

At USD, Burke is not quite as fortunate. The situation was tight. "We hired temporary workers to assist the telecom crew to pull the cable to meet our timelines," Burke says. He also wants more network staff.

"We are understaffed with two positions but will be adding two more soon," he expects. "I have advocated for more network staff specifically to maintain our wireless network since it is the preferred method for connecting with faculty, staff, and students," Burke adds.

The Bottom Line

WCU's budget for the project was the cost of the WiFi deployment. That price tag varied based on the locations, number of rooms, and access points.

Consulting services augmentation were provided by Aruba Networks of Sunnyvale, California, and Comm Solutions of Malvern, Pennsylvania—a local company.

Barimani says there were "substantial" cost savings on wired infrastructure costs. These savings came mainly from not having to deploy many switches and other savings in associated wired deployment. WCU figures that eliminating cabling costs and going all-wireless in the dorms gave them more than $1 million in total cost savings.

As a bonus, the IT staff can point proudly to the resulting reduction in carbon emissions contributing to WCU's striving to be a green campus. IT figures that in addition to dollar savings, its initiative let WCU reduce its carbon emissions by more than 100 metric tons due to reduced electrical consumption and wired-switch cooling costs.

Neither WCU nor USD levies any direct billing cost to faculty or students. At WCU, funds associated with technology improvements were used to pay for the project. In some cases, affiliated housing funds were assigned to deploy the WiFi technology.

"Our community is not charged for Internet access," Burke says of USD. "Our students are all wireless except for a few who still have gaming systems that do not have a wireless card built in," he adds. The wireless initiative continues.

"We submitted a request for two MCOs to fund the first two phases and will request another $1.2 million for hardware support," Burke says. "WiFi is the only way our students connect, and they demand high speed and expect reliable connectivity. It was easy to get funding," he concludes.

Concluding Thoughts

The name of the game is access, and the game continues. But with technology on their side, users are sure to come out on top.

Curt Harler is a contributing editor to the ACUTA Journal. *A freelance writer who specializes in technology issues, he can be reached at curt@curtharler.com.*

Attending ACUTA Events Promises an Excellent ROI

In this era of tight budgets, higher-education professionals must often prove the value of educational conferences before attending. We've pulled together some information that will help you demonstrate how attendance at ACUTA events supports your institution's goals.

ACUTA's educational programming is first rate. It allows you to:

- Learn first-hand from industry and higher-education experts who have successfully implemented technology solutions, avoiding costly and time-consuming mistakes.
- Create a professional network of knowledgeable peers and colleagues from other institutions
- Create talking points to communicate more effectively with vendors
- Get immediate answers and solutions to issues within your institution

The Exhibition allows you to:

- See the latest in technology and services, discovering new products that can decrease expenses and increase revenue
- Visit with current and prospective vendors in one location
- Get answers directly from vendors on the exhibition floor
- Comparison shop for the best value

Develop Your Agenda

Clarify the purpose of your attendance. List the things you would like to accomplish:

- Identify current issues at your institution for which you are seeking solutions.
- Research projects you anticipate in the future to get a head start.
- Inquire about developing technologies that might benefit your institution.
- Talk to your vendors about specific issues you are facing.
- Find one idea that will increase revenue and/or decrease costs.
- As your campus looks at implementing a new technology, you will attend sessions that will help you succeed with this implementation.

Make a Presentation to Your Management

You may wish to prepare a formal memo directed to the appropriate manager requesting attendance and why. The memo will be most successful if it focuses on what you will specifically bring back to the institution in return for the investment. On the ACUTA website, you will find a sample memo and the following talking points that may assist you in making the case to attend. It could read like this:

- ACUTA has been hosting national seminars for many years and serves its membership by providing two specific topics of interest at each seminar and covers an impressive list of hot topics at the annual conference.
- I am going to look for a solution for [this particular problem or issue].
- I believe [this new technology] could benefit the institution, and I would like to learn more about it.
- Our institution will benefit from contacts I make with other schools facing similar challenges.
- The educational sessions at ACUTA events are right on target with our institution's/department's current and future needs.
- Having so many vendors in one place at one time can reduce the time spent while at the office in researching and meeting with vendors, and I will share product information with you and my colleagues in the department when I return.
- I will share the slides from and links to educational sessions with co-workers when I return. (Slides will be available online.)
- I will write a report on highlights from the event and share the key takeaways at a subsequent staff meeting.

Join us for our next event, and you'll head home with a refined perspective on both current and future developments in IT and telecom that will benefit your institution for years to come. That's what we call ROI.

44th Annual Conference & Exhibition

April 19–22 • Atlanta, Georgia • Hyatt Regency

Contact Lori Dodson (ldodson@acuta.org) to register for the exclusive C-Level Strategic Leadership Forum on Monday

Fall Seminar

October 25–28 • Baltimore, Maryland • Hyatt Regency

Coming Soon to Your Campus: Wireless IoT

What impact will it have on your network?

by Gary Audin

The Internet of Things (IoT) has arrived on your campus or is coming soon. There are things you should probably know right now about IoT if you are going to successfully meet the challenges it is sure to present.

Defining IoT

The Internet of Things can describe a huge number and many types of endpoints, all of which can be passive, such as read-only devices and sensors, or active and able to report status, alarms, and alerts. Endpoints can also be used to control and change operations. The types of endpoints already in use can increase energy efficiency, reduce costs, and improve safety.

ABI Research estimates that there will be 30+ billion devices wirelessly connected to the Internet of Things by 2020 (https://www.abiresearch.com/press/over-2-billion-location-based-sensor-fusion-handse). Cellular networks will support many of the portable/mobile IoT devices, but there will be a huge population of fixed IoT endpoints that will need to communicate over short-distance wireless networks. IoT is going to affect networks.

IoT applications that may be of interest to educational institutions include:

- Building automation
- Energy management
- Lighting control
- Healthcare
- Advanced remote controls
- Telecom services

Wireless IoT Technology Choices

Each of the four potential wireless technology choices has its advantages and limitations. (See Figure 1.) When WiFi and Bluetooth emerged, IoT was mostly a concept. ZigBee was designed for a large population of low-power, low-bandwidth endpoints. Thread is a new entrant into the IoT space.

- WiFi is a LAN wireless technology that uses 2.4 GHz or 5 GHz radio and is widely deployed in both enterprise and consumer locations. It is the implementation of the IEEE 802.11 standards, 802.11 a, b, g, n. WiFi is best applied to sending large amounts of data wirelessly between devices and is a large energy consumer.

Many IoT endpoints require only a low level of data throughput. The bandwidth capabilities of WiFi exceed the requirements for the majority of IoT endpoints. If the WiFi endpoint runs with batteries, then the batteries have to be recharged or replaced in days; but most WiFi endpoints derive their power from PoE LAN switches, not batteries.

- Bluetooth technology was introduced by Ericsson about 20 years ago for personal area networks (PANs). A Bluetooth PAN transmits data over the frequency band between 2.4 and 2.485 GHz. Because it supports over shorter distances compared to WiFi, it can operate with less power. Devices like phones, smartwatches, headsets, speakers, and computers can be paired together. Bluetooth v4.0 delivers the ability to implement low-energy features that conserve power. Bluetooth devices don't communicate with each other. Version 4.2 introduces three low-energy updates to the specification: data packet length extensions, privacy upgrades, and secure connections. Bluetooth is not a candidate for mesh networks.
- ZigBee is a specification for a group of communication protocols used to create PANs that support low-power digital radios. It is based on an IEEE 802.15 standard that specifies transmission distances 10–100 meters line-of-sight. The ZigBee endpoints are commonly run off of batteries that have a long life, months to years, because of the endpoints' low power consumption.

The useful distance depends on power output and environmental characteristics. The lower two open systems interconnection (OSI) layers are defined by the IEEE standard (http://standards.ieee.org/about/get/802/802.15.html), and the ZigBee Alliance (www.zigbee.org) embraces the middle four layers. The top application layer can be defined by the ZigBee Alliance or a vendor producing a proprietary solution. The drawback to ZigBee is the number of different implementations making product interoperability problematic. ZigBee does support mesh networks.

- Thread is a newcomer to the IoT wireless network world. Thread is the product of an alliance that includes Nest, Samsung, ARM, and four other companies. The Thread Group plans to provide rigorous testing, certification, and standards enforcement. Existing Thread specifications would be able to support a network of up to 250 devices. Thread uses the same radio technologies as Zig-

Bee from the IEEE standard 802.15.4, and it supports mesh networks. Thread developers want to avoid what they see as the ZigBee problem of fractured standards by requiring a certification program or products. Look for its development, but it is not yet a major candidate for IoT.

Capacity/Performance vs. Coverage

The advent of IoT endpoints will change wired and wireless network designs, but a faster WiFi LAN will probably not be required to support the increased number of IoT endpoints. High-speed transmission is not what most IoT devices will need, so bandwidth is not an issue. The wireless LAN designer has to implement networks that will probably have a smaller physical coverage area, so more access points will have to be deployed. The number of endpoints communicating over the wireless LAN will significantly increase.

The traffic generated by the IoT endpoints will be small data packets, which can cause a decrease in the LAN efficiency because of the higher protocol overhead encountered. The LAN performance will need to be high in capacity (the number of IoT endpoints connected) as well as availability because a failure can seriously jeopardize operations. Only the endpoints that support emergency and alarm measurements would need QoS; the rest can effectively operate without it.

What Does the IoT Network Look Like?

The single biggest observation about IoT is the number of potential endpoints that will exist. IoT will also be a contributor to big data, and it is expected to deliver many benefits. For example, endpoints can initiate connections when they have a change in status or have an operational problem before humans will know, and inventory systems can monitor the inventory status independent of where the resource is located.

Organizations that appear to be early beneficiaries of IoT include healthcare, transportation, hospitality, mining, warehousing, and public venues such as stadiums and conference centers.

Figure 1. Comparing wireless choices

	ZigBee	Bluetooth	WiFi	Thread
IEEE standard	802.15.4	802.15.1	802.11 a,b,g,n	802.15.4
Battery life (days)	100 to 1000	1 to 7	1 to 5	100 to 1000
Network size	65+K	< dozen	Dozens	250
Bandwidth	20 to 250 kbps	700+ kbps	10–100s Mbps	20 to 250 kbps
Transmission range	100+ meters	10 meters	100 meters	100 meters

In the past, wireless network designers have been more concerned with the physical coverage area than with the number of wireless devices supported. IoT will change all of this. Where coverage area was the goal, now capacity and performance are driving design.

Challenges of Wireless IoT

IoT will have an impact on both employees and students. The network challenges are many as there will be a significant increase in the data communicated as data traffic grows exponentially. Traffic will be very unpredictable—consider an announcement at a public venue that causes data to explode but only during the public event.

The number of endpoints to support simultaneously will also continue to grow, and the traffic generated by these endpoints will probably grow at a faster rate than the addition of endpoints, in effect multiplying the traffic. Some other implementation concerns include:

- Security
- Access control
- Scalability
- Endpoint management
- Capacity management
- Troubleshooting problems both with the network and endpoints

The network designers will have to balance coverage with capacity and deliver capacity that can deal with wide fluctuations in traffic without bringing down the wireless network. Applications on the network will have to be involved in controlling traffic so that the network will not be overwhelmed. Today, most application designs assume that there is always capacity available. Application designers will have to employ some form of traffic throttling within their applications to help the network manage traffic bursts.

Comparing Choices and Solutions

There are three common mature choices for connecting to wireless endpoints over short distances of generally 100 meters or less: WiFi, ZigBee, and Bluetooth. The choice for IoT has to be able to support many endpoints in a limited area. The data produced by IoT endpoints in most cases are modest; therefore, the bandwidth required is also modest—kbps not Mbps. ZigBee can support a far greater number of endpoints than either WiFi or Bluetooth can, but neither WiFi nor Bluetooth was designed for high-density, large-endpoint populations. (See Figure 1.)

WiFi is best suited for desktop, laptops, tablets, and phones that require high data rates. Each of the added 802.11 standards has been directed at increasing bandwidth. Bluetooth was designed to deliver service on a desktop connecting a wireless keyboard, mouse, printer, or headset. When both the supported population and the area coverage are large, then ZigBee and Thread become the preferred solutions.

Processing IoT Data, Impact on the Networks

IoT traffic comes in many forms. An IoT message can be triggered by an event or alarm or can be streaming constantly. Most of the data packets will be small. Other than streaming, most IoT data will not require much bandwidth.

ZigBee and Thread network devices can communicate in a mesh network where any device can talk to its neighbor. WiFi is primarily used to connect to an access point that then connects to an IP network. Bluetooth can talk among a few nearby devices but is not often connected directly to an IP network. There will be a connection point for both ZigBee and Thread devices to connect to an IP network. The connection point can be an IP WAN network router or a cellular service access point.

Currently, collection of IoT data is typically centralized—for example, a data logger that stores temperature and humidity or the use of building entrances and exits. The analysis of that data must be centralized, especially as you move up the analytics maturity curve to gain operational intelligence from the data.

As sensor technology advances, we will start to see ecosystems where limited analytics can be decentralized. Some companies already offer endpoint controllers that process and digest IoT data. There will be less traffic carrying less data, data that is the result of decentralized analysis. Decentralized processing will reduce the traffic on the IP WAN and over the cellular networks but will not reduce the traffic on the internal wireless networks.

Who Should Manage IoT?

When you look at IoT, the endpoints deal with operational issues, not IT issues. The endpoints will most likely provide information for managing non-IT resources. There is a movement for the operations side of the institution to install, maintain, and administer the IoT endpoints, not IT. This is called "operations technology" (OT). In some retail implementations of IoT, IT has been bypassed at IT's request. The IoT data can also be analyzed in cloud services that already exist for building automation, transportation, and retail operations, thereby eliminating any burden on IT. The institution may see a separate OT budget in the future.

Final Thoughts

The Internet of Things is going to raise the bar on technology changes significantly in the near future. There is a lot to learn if we are to successfully maneuver the new technology landscape.

Consultant Gary Audin is a principal at Delphi, Inc. He has many years of experience in communications technology and is a frequent contributor to ACUTA publications. Some portions of this article have been posted at www.nojitter.com and www.webtorials.com.

IoT Expert Observations

In an article by John Dix in *Network World* (2/10/15), four IoT experts made some salient points about IoT:

David Mattes, CTO, Tempered Networks: In the early days of networking, you had extreme heterogeneity of protocols, and it was the convergence of those protocols that created the security problems and the security industry we have today. Similarly, we've been doing IoT-type things since the 1980s with an alphabet soup of protocols. With IoT, we will see the same thing; we'll have a convergence at some point to a more homogenous environment, and that's going to cause the next security crisis.

Ari Jules, Professor in the Jacobs Institute at Cornell Tech: We may see a striking shift in our social attitudes toward ownership of data as the custody of personal data from like fitness trackers and medical devices and so forth is taken by service providers and not necessarily made available back to the customer. Should an individual own his or her own heartbeats? The answer would seem obvious, but in today's environment it's not so clear. If you're wearing a fitness tracking device and all of your data is uploaded to the servers owned by the fitness device provider, it's not guaranteed you'll get access to the data, and in many cases, data can be resold. So we're seeing a loss of ownership of data that would seem to carry a fundamental right of possession.

Marc Blackmer, Product Marketing Manager, Cisco: IoT is the Wild West right now. We don't know what it's going to look like, where it's going. We're right at the cusp and, while there's a lot of opportunity, there is an intrinsic vulnerability because too often security is bolted on after the fact. So what concerns me is a rush to market to take advantage of the opportunities and not building in the necessary security and privacy protections, meaning we have to patch that together down the road.

Patrick Tague, Associate Director, Information Networking Institute, Carnegie Mellon: There's nothing we can do to stop this. It's already providing some value, and that value is likely to outweigh all but the most catastrophic developments. I do think that a certain amount of regulation is going to become necessary, especially given things like those autonomous vehicles, and my prediction is there will be a lot more regulation of IoT once we have our first major software-based real-world disaster.

The Federal Research Grant and FISMA Compliance

Six steps bring you into compliance

by Kevin W. Shaffer

The Federal Information Security Management Act of 2002 (FISMA, 44 U.S.C. §3541 et seq.) is a United States federal law enacted as Title III of the E-Government Act of 2002 (Pub.L. 107-347, 116 Stat. 2899) requiring all federal agencies to document and implement security controls designed to protect information and information systems that support their operations and assets. FISMA also delegates the National Institute of Standards and Technology (NIST) to develop and publish standards and guidelines that assist agencies and organizations in determining their optimum information security posture for the protection of their operation and assets.

Federal agencies or any entities on behalf of a federal agency are required to (1) develop, document, and implement an information security program and (2) provide information security for the information and information systems that support the operations and assets. Universities with research departments that receive federal grant or contract funding may be directly impacted by FISMA. If the grant or contract requires the university research organization to return data to the federal sponsor or if the research organization obtains federal funds using a federal contracting form, that research organization must be FISMA compliant. The law requires a minimum set of security controls to be in place and a formal audit conducted prior to obtaining an Authority to Operate (ATO) and a continuous monitoring process be put in place to verify ongoing compliance.

Relevance to Research

An April 2010 Office of Management and Budget memorandum requires federal agencies to report their FISMA compliance to Congress. In addition, the memo requires all contracts involving sensitive data, as well as grants where sensitive information is created, accessed, or stored on behalf of the federal government, be covered under FISMA.

Federal funding of university research may obligate the research recipient to have a FISMA-compliant information security program in place. The research funding contract or grant language often indicates if, in fact, compliance requirements apply. Federal agencies may vary their introduction of FISMA-compliant language into contracts, grants, or initial RFP by referencing OMB A-130, FIPS 199 or wording such as "...will comply with all applicable NIST standards..." Statement of Work documents may include FISMA-compliant language in plain and simple terms or include references to the System Security Plan (SSP), Security Assessment Report (SAR), and the Plan of Action and Milestones (POA&M) report. FISMA-compliance requirements may also be inserted in contract modifications and renewals issued in 2010 or later.

Compliance with FISMA benefits the university and its research department by helping to provide for the continued flow of funds, securing future research funding, and protecting the university's research reputation.

The consequences of non-compliance on a university's research program and the university itself are substantive. If FISMA is controlling as a result of the grant or contract, compliance is mandatory, and research funding may be withheld or terminated in the event of non-compliance.

NIST

NIST provides a series of Special Publication documents directed at guiding an agency or enterprise through the processes leading to FISMA compliance. NIST is tasked with the development and publication of guidelines and standards for FISMA compliance and a wealth of security documentation exists, not only for guidance in FISMA compliance, but to serve as reference documents for a wide range of information security–related issues.

Six Steps

FISMA compliance is attained via a six-step cyclical process that is part of the Risk Management Framework (RMF). The RMF process recognizes a shift from policy-based compliance to risk-based protection. Enterprise missions and business functions dictate security requirements and the safeguards or countermeasures implemented. An enterprise risk evaluation should precede the six-step process outlined below.

1. Categorization

In the first step, the organization defines the sensitivity of information and information systems using risk assessment processes, applying a matrix that determines the low, moderate, or high risk level of data and systems regarding

confidentiality, integrity, and availability. It is considered the most important element in the RMF process.

The authorization boundary is also determined in the initial categorization step. The boundary encompasses all the components of the information system and the perimeter defense DMZ line enclosing the system and sensitive data. The authorization boundary is determined by identifying the information resources needed, avoiding a boundary too expansive or limited and keeping the boundary realistic and cost-effective. System and data description and categorization, an overview of security requirements, and a description of agreed-upon security-related materials are documented in the System Security Plan (SSP). NIST Special Publication (SP) 800-60 provides mapping tools for information and information systems to security categories by identifying information types, selecting provisional impact levels, and assigning system security categories.

Security needs to change perception, change the language, to bring security more in line with academia—not in terms of security provided but in terms of shared goals, collaboration to facilitate, not prevent.

2. Selection

The second step includes the selection of baseline and supplemental security and privacy controls and any appropriate tailoring of selected controls based on the prior risk evaluation. Controls come in three varieties; common, specific, and hybrid. Common controls can be applied enterprise wide. Specific controls have a narrower, system-specific application. Hybrid controls use a combination of common and specific.

There are 18 control families—such as Access Control, Identification and Authentication, Awareness and Training, System and Information Integrity, Incident Response—with mapping to ISO/IEC 15408 controls. After determining the common, baseline, and supplemental controls, the selections and monitoring strategy are documented in the SSP in addition to control identification explanation and agreements established between systems sharing data. NIST SP 800-53 Recommended Security Controls for Federal Information Systems and Organizations provides guidelines for selecting security controls.

3. Implementation

The next step is the implementation of the selected security and privacy controls and configuration settings using sound systems-engineering practices within the enterprise architecture. The implementation details should be documented, including functional descriptions of inputs, expectations, behavior, and discernable implementation impact.

4. Assessment

Assessment determines the security or privacy control effectiveness, proper implementation, proper operation, and if the controls are meeting the security and privacy requirements for the system. The assessment is a risk-based process in which performance is dictated by scope and cost, which in turn may determine whether the assessment is conducted in-house or by a third party.

The degree of independence required in an assessment is another significant factor determining who conducts the assessment. Specific security objectives are evaluated, and comprehensive testing of selected security and privacy controls for vulnerability and risk are conducted. Assessment preparation includes development, review, and approval of the assessment plans and controls to be assessed. The actual assessment is conducted in accordance with the assessment procedures defined in the security or privacy assessment plans, which may be combined in one plan.

Testing, interview, and examination constitute the assessment methods utilizing the associated attributes of depth and coverage which help define the level of rigor and scope for the assessment. The assessment depth attribute directly corresponds to the testing, interview, and examination processes which include basic, focused, and comprehensive formats. Basic, or black-box testing, provides the assessor no system knowledge prior to the assessment. Focused, or grey-box testing, allows for limited system knowledge; and comprehensive, or white-box, testing provides explicit system knowledge at the time of the assessment. The assessment coverage attribute relates to the breadth of testing, interview, and examination.

The results of the assessment will determine any immediate remedial action taken regarding the security or privacy controls. All assessment plans, security and privacy assessment reports, findings, and recommendations are documented in the Security Assessment Report (SAR). Both NIST documents SP 800-53A Guide for Assessing Security in Federal Information Systems and SP 800-115 Technical Guide to Information Security Testing and Assessment are available for facilitating the assessment process.

5. Authorization

The Assessment and Authorization process, if concluded satisfactorily, results in an Authority to Operate (ATO). The ATO is issued based on a determination that the risk to organizational operations and assets is acceptable given the security posture of the agency or enterprise. The Authorization Package is assembled, consisting of the SSP, the SAR, and the POA&M, a report based on findings and recommendations of the SAR. The Authorization Package is presented to the authorizing official (AO) for consideration of the ATO. The AO will typically be the project or grant sponsor. The ATO is a formal authorization decision with terms and conditions for authorization and an authorization deadline. With risk

determination and acceptance completed, an approval letter accompanies the ATO as initial authorization, ongoing authorization or reauthorization. NIST SP 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems details aspects of the authorization process.

6. Continuous Monitoring

The most recent revision to the RMF process involves this last step, transitioning from monitoring to continuous monitoring, which provides for the uninterrupted tracking of changes to the information system that may impact security controls and reevaluation of control effectiveness. Information Security Continuous Monitoring (ISCM) includes defining an ISCM strategy, establishing ISCM metrics, implementation of the ISCM program, analysis of the program, response to findings, review and update. Three NIST documents should be consulted for continuous monitoring issues: SP 800-37 R1 Guide for Applying the Risk Management Framework to Federal Information Systems, SP 800-53A Guide for Assessing Security in Federal Information Systems and SP 800-137 Information Security Continuous Monitoring.

Where existing controls are in place and a low-security category selected, a limited project can be accomplished in a short time frame. At a moderate risk level, a large or elaborate project may extend beyond a 12-month period. The process length is usually determined by the security category selected, availability of resources with skills and time to manage the process, current level of security controls, number of participants, and the complexity of the computing environment.

In December 2014 the 113th Congress passed the Federal Information Security Modernization Act, a long-anticipated FISMA update. The new legislation will provide for clarification of roles and responsibilities for the Office of Management and Budget and the Department of Homeland Security (Section 3553), implement more automated processes relieving burdensome paperwork demands, and improve transparency and accountability via data breach management and reporting (Sections 3554-3559). The OMB will have six months to eliminate inefficient and wasteful reporting processes by revising Appendix III of the A-130 circular.

Additional information regarding the risk management process can be found in NIST SP 800-39 Managing Information Security Risk. Special Publication 800-53 Appendix H Security Control Mappings for ISO/IEC 27001: 2013 update was released on August 28, 2014, to maintain consistency with the 2013 revision to ISO/IEC 27001. Prior to the H Appendix revision, on July 31, 2014, NIST released an update to SP 800-53A Assessing Security and Privacy Controls in Federal Information Systems and Organizations. This update contained important changes to the 2010 version of the publication.

A Saleable Vision and Buy-in

While FISMA compliance appears to be a daunting task, the process can be handled in a much more transparent and efficient manner if pre-existing university infrastructure can be utilized. Having an authorization boundary that meets a broad range of regulatory requirements simplifies the compliance process ,allowing for a more productive and economical approach.

Having established an authorization boundary that is expansively compliant in terms of regulatory conformity, FISMA-HIPAA, a university has gained an effective tool in bringing on board stakeholders across the campus and research community. A previously defined and established explicit security parameter utilizing firewall protection and intrusion detection/prevention methods, applying encryption where appropriate, securing the data at rest and in transit, allows for a more robust approach to meeting increasing compliance requirements.

Security and Academia Handshake

In addition to providing an incentive to the university and research community by offering a pre-existing secure digital storage area that transparently meets compliance requirements, the higher education security community can help promote a more conciliatory mood by tailoring its security approach.

Quite often the university and research community are at apparent odds with the security office, one vying for a more open and inclusive data access point of view while the security perspective is seen as restrictive and cumbersome. The university community interprets security implementation as a preventative to flexible data access and data sharing. The need is for data to be accurately preserved, for contemporary use and for future generations, accessible to those who need the information. The goals of academia and security are the same but the language of security can conflict with that of academia.

Security needs to change perception, change the language, to bring security more in line with academia—not in terms of security provided but in terms of shared goals, collaboration to facilitate, not prevent.

Both entities are striving for the same outcome, the confidentiality, availability and integrity of the data being preserved, and compliance is the enabler.

University research entities will find the FISMA requirements less intimidating and be more likely to embrace compliance and thus secure their federal funding if the pathway to FISMA compliance is already paved and well maintained, and adequate communication, reasoning, and purpose well posted along the route.

Kevin Shaffer is Information Security Analyst /Data Security Policy and Compliance, at the University of Cincinnati. Reach him at kevin.shaffer@uc.edu

Managing Privacy and Security in the Age of IoT

Proceed with caution as we transition to global connectivity

by Martha Buyer

As the volume of information about absolutely everything we do becomes increasingly large, and as the number of recent data security breaches continues to climb, large consumers of telecommunications services have tried to be increasingly vigilant about staying current on the latest and greatest techniques for managing potential privacy and security breaches. Most Americans are familiar with horror stories of the recent major data breaches that have hit the headlines in a big way and think quietly to themselves something along the lines of "there but for the grace of God…" (you know the rest). Target and Anthem come to mind immediately, but there are legions of others.

> *"The real power of the Internet of Things is that it transforms a static product into a dynamic service."*
>
> *Jahangir Mohammed*

Consider the fact that these major corporations make an effort to use current relatively state-of-the-art detection and monitoring systems, and even *they* have been infiltrated with current malware. Should you be concerned? Absolutely. But wait. There's more.

Now consider the routers you use at home or in lower-profile parts of your operation. How old are they? In many cases, the honest answer is at least several years old. Based on the age and sophistication of all of existing network components, the information stored on—or traveling over—the network is vulnerable not just to the type of threats that have affected the Targets and Anthems of the world, but also to very real threats that are years old and correspondingly much less sophisticated than those currently making the rounds. Think of the adage "a chain is only as strong as its weakest link." Be concerned. Very concerned.

The FTC Steps In

Aware of these obvious vulnerabilities made all the more acute by the explosion of the IoT, the Federal Trade Commission has taken action. (Its report, which was released in January, can be found at www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.)

FTC chair Edith Ramirez is motivated by the fact that the privacy and security concerns created by the rise of the IoT have the potential to undermine consumer (you can easily insert the words "student," "faculty," or "staff") confidence in a significant way. "The only way for the Internet of Things to reach its full potential for innovation is with the trust of American consumers," she said recently. Commissioner Ramirez believes that technology innovation is only a good thing if consumers are confident that they won't be the next victims of a high-profile breach. If this heretofore private information is readily accessible to the immediate world, and what was thought to be private is now public, consumers have good reason to be alarmed in general and distrustful of the companies that manufacture, distribute, and sell such goods and services.

In its report, the FTC made several important suggestions to mitigate consumers' concerns. First, the Commission encourages manufacturers to ensure that security is built into devices as they're made, rather than after they're already on the market. Second, the agency suggests that all employees be instructed on the importance of information security, and that security issues have a sufficiently high profile within the manufacturing/selling organization to keep them front and center at all times. Although there are other suggestions, the last uber-critical one is that devices be monitored throughout their anticipated life cycle (think home routers) such that security updates and patches are provided at all times to cover known and newly discovered risks regardless of the age of the device.

In addition, the FTC also suggests that companies in this space consider "data minimization," the practice of limiting the collection and retention of consumer data for a set period of time only, and never indefinitely. According to the FTC, data minimization has two goals with respect to privacy: first, accepting the risk that a company with a large store of consumer data is "a more enticing target" for data thieves or hackers based upon the volume of data that it has; and second, an acknowledgment that "avail-

able consumer data will be used in ways contrary to consumers' expectations." Finally, the FTC suggests strongly that companies selling IoT items to consumers educate those consumers about their reasonable expectations of what information is being collected and stored, and for what period of time.

Jahangir Mohammed, chairman of the Silicon Valley–based tech company Jasper, said in a recent interview that "The real power of the Internet of Things is that it transforms a static product into a dynamic service. Once a thing is connected, it really becomes unlimited in terms of what it can process, because it can borrow from all the computers in the Internet to do the processing, and it has real-time access to all the information in the Internet. It's no longer an isolated thing. It's become part of a fabric of everything connected. It's a part of a much larger fabric. It's a service. This is the real power of the Internet of Things."

The Application to Campus

So how does this apply to a campus environment? Mark Reynolds, ACUTA's current president and the associate director of IT at the University of New Mexico ("everyone's a Lobo, woof, woof, woof"), commented recently that "we sit fat and happy and negotiate a contract and buy a product, and then everyone forgets what the contract terms are, and what the license agreement says about important things like renewal, upgrades, and ongoing maintenance. Then we have a problem, and suddenly, because everyone was so busy keeping the lights on, we're not looking down the road three years. Only when something goes wrong do we discover that the device/service is at end of life or needs support that has long since expired. And then we're doubly vulnerable—both to vendors who come to us and say 'Oh yes, here's your renewal, sign now or else' and to outsiders trying to weasel into our networks/devices that we thought were secure."

Reynolds suggests the creation and ongoing maintenance of an information repository, containing information about renewals, updates, and any other information regarding the licensed product or service. "The repository should contain triggers that could be set to time not only with contract terms, but in alignment with budget cycles so that we are forced to look and plan ahead for these renewals. Once there's a problem, it's too late. We need to know in advance so that we can manage both the practical aspects of an unanticipated problem and the budget process so that we can manage providers in the best way that we can."

Final Thoughts

The additional information that's generated by the IoT is no doubt powerful. But with great power comes great responsibility—on the parts of the manufacturer, distributor, retail outlet, and, ultimately, the consumer. Privacy and security experts encourage consumers, in the strongest possible terms, to consider the risks and consequences before sharing seemingly harmless information with the immediate world. I couldn't agree more.

Martha Buyer is an attorney whose practice is primarily focused on telecommunications law. Her practice is a certified New York Woman-Owned Business. She is also a frequent contributor to No Jitter (www.nojitter.com). She can be reached at martha@marthabuyer.com.

visitbaltimore.com

Coming ACUTA Events

Mark Your Calendar!

Fall Seminar
October 25–28, 2015
Baltimore, Maryland
Hyatt Regency
Track 1. Preparing & Innovating for Tomorrow
Track 2. The Business of IT

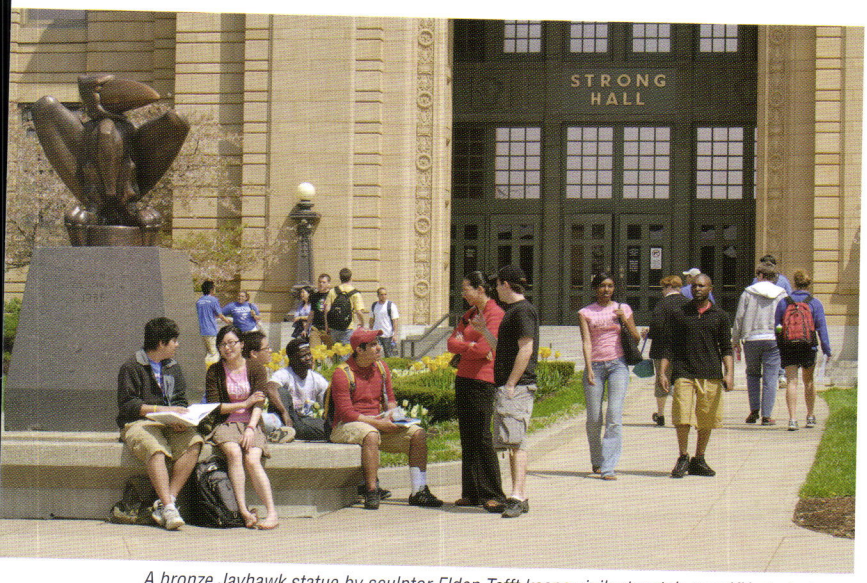
New Orleans CVB: Richard Nowitz

Winter Seminar
January 17-20, 2016
New Orleans, Louisiana
Hyatt Regency
Topics to be announced

Visit the website for details: **www.acuta.org**

Institutional Excellence Award 2015

Reorganize and Redefine KU IT



A bronze Jayhawk statue by sculptor Elden Tefft keeps vigilant watch over KU students on the University of Kansas Lawrence campus.

Great technology organizations don't start with technology. Rather, success begins with a focus on their customers and the employees who serve and support them. Success is also determined by an organization's willingness to do the right thing for their customers, knowing the choice may mean more work and a steeper climb. Implementing a vendor solution is a complex and challenging endeavor, but a different kind of innovation is needed to re-imagine, reorganize, and redefine an established technology organization. When technology organizations seek to innovate in areas that matter as deeply to people as jobs, funding, control, and institutional history, there is inherently tremendous risk; but over the past three years, KU Information Technology (KU IT) at the University of Kansas has proven that when this is done well, the rewards far outweigh the challenges.

Reorganize and Redefine KU IT

KU IT has developed and implemented a new technology-support model designed to improve customer service, ensure consistency and compatibility in services and systems across campus, provide operational savings, and create new career growth opportunities for campus technology staff. The outcomes for the "Reorganize and Redefine IT" initiative met or exceeded original expectations, and the process has allowed the organization to grow and develop in new and exciting ways. Through the implementation of a new "locally supported and centrally managed" technology-support model and related centralization projects, KU IT provided significant benefits to its customers, campus technology staff, and the university overall. Through the process, KU IT fundamentally improved as an organization, bolstering its reputation as a trusted campus partner and establishing KU as a leader in organizational change.

Like many tier-one research universities across the country, information technology at KU grew organically as computers and the technology industry evolved. This emergent process resulted in the inefficient dispersion of technology staff and resources in individual units (i.e., schools and departments), and a lack of central management and no comprehensive, campuswide strategy. Unit administrators took on the management of both technology staff and the implementation of new technologies. And because there was no comprehensive strategy or coordination, little thought was given to how new solutions would integrate with existing technologies on campus. This silo effect also led to duplicated services and a loss of collective bargaining power for vendor purchases.

Over time, the real impact of a decentralized support model could be seen most in the missed opportunities to improve teaching, learning, research, and the campus experience as a result of the inability to implement integrated technology solutions across the entire institution.

To support KU's 5-year strategic plan (launched in 2011), university leaders identified a number of initiatives to improve efficiency and save operational costs, which could then be reinvested in strategic priorities. Reorganizing and redefining the role of decentralized IT staff at the Lawrence campus was one of several initiatives focused on improving the efficiency and effectiveness of technology resources across the university. By centralizing the management of all technology services and support functions, associated personnel and expenditures, KU IT could improve customer service and provide cost savings that could be redirected toward the academic and

research mission of the university.

At the start of the project, KU IT faced two major hurdles. First, some campus customers viewed KU IT as an inconsistent organization in need of a more clearly articulated strategic plan and vision. Before KU IT could move the university forward with a culture-changing solution, it first had to look inward and become a more strategic and customer-focused organization. Second, beliefs about centralization and natural apprehension about organizational change made it even more imperative for KU IT to establish itself as a trusted campus partner.

Under new leadership in fall 2011, KU IT took decisive steps to become a more customer-focused and professional organization. KU IT leaders began to articulate a clear vision and instituted new practices that allowed for more consistent support and services. The organization also began an on-going practice of more broadly listening to all stakeholders and communicating the results and outcomes of major efforts with partners and university leadership.

Over the life of the Reorganize and Redefine project, KU IT remained focused on changing the perception of the organization by demonstrating accountability and transparency. As the organization became more open and accountable, relationships improved and trust grew with partners across campus.

Planning, Leadership, and Management Support

The locally-supported-and-centrally-managed model is a true collaboration between KU leadership, KU IT, and partners from across the institution. Because the efforts to reorganize and redefine IT support on campus are directly aligned with the institution's vision and five-year strategic plan, the project had early buy-in and on-going support from top leaders.

The scope of this on-going, multi-year, multi-phased project is substantial, involving hundreds of employees and 19 campus units (schools or departments) to date. Work began in 2011 with a comprehensive look at KU IT and thorough exploration of the ways the organization could change to better serve its customers. In parallel, there were regular interactions with university leadership, including deans, directors, staff, the chancellor, the provost, vice provosts, and vice chancellors, to better understand the vision, strategy, needs, and pain points of each unit on campus. Success required active participation from across the entire university.

In 2012, KU IT formed project teams that included KU IT leadership and departmental staff, campus partners, and external advisors. Guided by an evolving customer-first philosophy, the teams worked to identify opportunities and risks for the initiative. Together they reviewed the pros and cons of centralized and decentralized support models and designed a hybrid model that capitalizes on the best aspects of both. Having technology support staff located in campus departments with their faculty and staff customers was among the most valuable aspects of the decentralized approach. That's why in the new locally-supported-and-centrally-managed model, technology staff members remain in their current locations, while reporting to central IT through managers at newly formed Technology Support Centers (TSCs).

Leaders in the partner units work with their TSC manager and KU IT's Deputy Support Officer to propose and prioritize technology projects and provide input into the performance of the IT staff supporting their unit. KU IT is then responsible for providing the most effective technology solutions to fulfill the business or academic needs of the unit.

For each campus unit, the process for implementation begins with an assessment of the current personnel and resources, along with an evaluation of their specific customer needs. In each case, workstation and server support, application and web support, and classroom and lab support are assessed to get a holistic view of the technology in the unit and identify duplicated services and potential cost savings. Finally, a master service agreement (MSA) is negotiated for each unit, which clearly articulates expectations and deliverables. With the MSA complete, funding lines for technology staff positions are transferred from the unit to KU IT and departmental technology staff begins reporting to KU IT.

Promotion of Technology and Maturity of Effort

In the past three years, KU IT has successfully partnered with 19 of 22 campus units to provide technology support under the new model, and is currently in discussions with leaders of the other three units. KU IT worked closely with leaders in each unit to develop individualized master service agreements that address their specific needs and priorities. The new model has fundamentally changed and improved how KU IT delivers technology support and services on the KU campus. Now there is a single point of contact for all technology needs for the units. As a result of this dialogue among units, TSC managers, and KU IT departments, KU IT is better able to incorporate the feedback and priorities of campus partners in university-level technology decisions. The new model allows for enhanced sensitivity to local needs and processes; service-centric decision-making; unified systems, policies, and procedures; and greater sharing of IT knowledge and resources across the university.

Even after building stronger relationships and trust on campus, asking unit leaders to relinquish a degree of control was not easy. Neither was convincing technology staff that giving up some of their autonomy would ultimately make their lives easier and help them advance professionally.

To overcome these challenges and further enhance the perception of KU

IT as a trusted partner, the organization remained focused on accountability and transparency through open and meaningful communications.

Before approaching units directly, KU IT began strategic communications efforts to build awareness of the initiatives among faculty, staff, and students. At the same time, KU IT leaders and project team members met with the stakeholders who would be affected by the changes. They listened, and sent direct and targeted communications to these groups that addressed frequent questions and focused on the benefits to individuals, departments, and the university.

The University of Kansas Lawrence campus is located on Mt. Oread in the center of Lawrence, Kansas.

What is perhaps most significant about this project is the fact that KU IT was able to achieve the university's cost and efficiency goals for the initiative by focusing on the needs of partners and employees and delivering a higher standard of service. This project proves that thoughtful, people-centered approaches to organizational change can yield enhanced trust and partnerships in addition to financial gains and improved business processes.

Quality, Performance, and Productivity

Operational cost savings was the only formal key performance indicator (KPI) for the larger Reorganize and Redefine KU IT project. To better serve its customers, KU IT leadership and project teams developed their own KPIs for the Reorganize and Redefine IT initiative specific to the TSCs that were created by the project. These KPIs include:

- Customer satisfaction
- Total number of help tickets
- Average time to assign ticket to staff
- Incident resolution, whether it met the service agreement
- Total first-call resolution (i.e., problems resolved on first call) maintained or improved
- Average time to resolve/close ticket

KPIs are communicated to partners via the MSA for each unit, and results are reported to university leadership. To date, expectations for all project KPIs have been met or exceeded. Additionally, KU IT has identified and implemented more than 300 business process improvements (BPIs) since the beginning of the Reorganize and Redefine IT initiative in 2011.

Cost, Benefit, and Risk Analysis

The resources required for this project were significant, primarily in the area of staff time related to project teams, partner engagement, and communications. KU IT identified numerous risks and challenges, including the following:

- Build trust and relationships with customers and campus partners
- Overcome concerns about impact on jobs (e.g., layoffs, salary cuts, etc.)
- Overcome distrust and perception of IT imposing the change on other units
- Resistance to change
- Service levels must be maintained or improved rapidly after implementation to prove change positive and protect partnership status
- Overcome perception that centralization of management equals standardization, loss of local priorities
- Overcome concerns of departmental IT staff who experience change in reporting structure, and build relationships and loyalty with new managers
- Continued inconsistencies in service and continued incompatibility of systems across campus if new model is not implemented
- Degree of complexity and need continues to grow if decentralized model persists

Overall benefits of the initiative include:

- Improved standard of service across the university
- Operational cost savings
- Improved governance/collective bargaining power on enterprise software licensing and hardware purchases
- Customer-centric decisions
- Streamlined processes and efficiencies gained
- Consolidation of knowledge
- Enhanced perception of KU IT as a trusted campus partner

In practice, the benefits of the locally-supported-and-centrally-managed model include benefits on four levels:

1. Benefits for the university
   - Efficiency in support and procurement

- Greater consistency in service and increased technology compatibility across the institution
- Cost savings through the elimination of competitive hiring of existing technology staff among departments within the university
- Cost savings through avoidance of duplicated services, systems, software, facilities and operating costs

2. Benefits for IT staff transitioned into new TSC model
   - Career advancement opportunities
   - Training and professional development
   - Back-up from other support staff for vacations and other absences
   - Increased access to central IT resources
   - Ability to escalate issues through tiered support system
3. Benefits for units
   - Consistent technology support
   - Increased access to IT resources
   - Improved ability to communicate local needs/priorities to central IT
   - Joint authority for technology decision-making between units and central IT
   - Knowledgeable back-up staff to cover primary IT staff absences
   - Cost savings through reallocation and cost avoidance
   - IT support for schools/departments that lack funding
4. Organizational impact for KU IT
   - Enhanced reputation as a trusted partner on campus
   - Ability to correct/avoid inconsistencies in services
   - Ability to correct/avoid compatibility issues between systems
   - Partnerships with deans/unit leaders and schools/departments pave the way for future collaboration
   - More responsive to local needs and priorities/processes

Customer Satisfaction/Results to Date

The Reorganize and Redefine IT initiative shows how aligning IT initiatives with the university's strategic plan through a customer-focused approach can drive institutional excellence and provide lasting benefits for the university, employees and, most importantly, individual customers.

As a result of the new locally supported and centrally managed model, faculty and staff at KU have seen improved service and response rates as the tiered system allows local support staff to escalate issues and get help diagnosing and resolving the toughest problems. Post-service surveys show that on average approximately 95 percent of KU IT's customers "agree" or "strongly agree" they are satisfied with the service they received. First-call response rates in most cases are about 85 percent or above—well exceeding the industry average.

The university has gained improved efficiency in support and procurement and has seen significant cost savings from the avoidance of redundant operating costs, equipment purchases, and elimination of competitive hiring of IT staff between units within the institution.

Technology staff in campus units, who often worked alone before the change, now have much-needed back-up for vacations and unplanned absences, access to far more resources—including system and application experts—and new professional development and career advancement opportunities. No employees were laid off as a result of the new model, and a number of previously decentralized staff have already experienced professional advancement through promotions to management positions in the new Technology Support Centers.

The immense success of the project is unquestionably a result of the direct involvement of KU IT's campus partners in both the planning and implementation stages, and the unwavering support of university leadership. With the help of this coalition of campus partners and KU leaders, project outcomes have met or exceeded initial expectations on all measures.

Thanks to a thoughtful planning and development process, there were virtually no unanticipated challenges. Leaders from partner units have been overwhelmingly pleased with the results and have shared their experiences with others.

News of KU's innovative approach to organizational change has started to spread beyond campus. A number of peer institutions have reached out to KU IT to learn about the support model and implementation process.

As a result of the project, KU IT has fundamentally improved as an organization. It has solidified its reputation as a trusted campus partner through improved business processes and a demonstrated commitment to putting customer needs first.

Centralizing management of IT support and services is an organizational challenge that many institutions of higher learning will face in the coming years. This kind of project is complicated and deals with essential topics that matter to customers and employees of the institution: jobs, funding, control and institutional history. These fundamentally human concerns can be seen only as risks to be mitigated, or they can be viewed as invaluable opportunities to elevate and enrich an IT organization's role as a trusted partner. This project demonstrates that in addition to financial and process successes, how an organization chooses to address the necessary changes will largely determine whether the project significantly enhances, or detracts, from the perception of IT at the institution.

For more information, contact David Day, Director of IT External Affairs, at itcoms@ku.edu or ACUTA primary representative Jaci Matney, Director of Enterprise Project, Program and Portfolio Management, at jaci@ku.edu.

Advertiser's Index

★ Indicates ACUTA Corporate Affiliate

By advertising in the *ACUTA Journal,* these companies are not only promoting products and services relevant to information 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.

Reach Higher Ed Clients with an ad in the *ACUTA Journal!*

For complete details contact Amy Burton, Director, Strategic Relationships

Phone: 859/721-1653 • e-mail: aburton@acuta.org

www.acuta.org

Be a part of ACUTA history...

Write for the Journal!

The ACUTA Journal Wants YOUR Story!

For 18 years (that's 74 issues now), the *ACUTA Journal* has brought you the insights and experiences of campuses from coast to coast about every imaginable topic of relevance to higher ed technology. We consistently hear that campus case studies are the most useful articles of all. You like to know what others are doing—what has worked and not worked—to help you make important decisions.

Has your campus implemented a new procedure or a new strategy?

Have you discovered a shortcut that might benefit others?

Is there an application or program that resolved some really tough issue for you?

The next two issues of the *Journal* fwill consider some very interesting topics:

- **Summer: Clouds in the Forecast**
- **Fall: Collaborating and Partnering for Success**

You are cordially invited to share your own campus story with other members via the *ACUTA Journal*. If you don't have time to write it, just **contact editor Pat Scott at pscott@acuta.org,** and she will connect you with someone who will work with you to get this done.

It's an opportunity for excellent visibility and recognition for your school, your department, and yourself.

ASPIRE TO LEAD

ACUTA 2015
Association for College and University Technology Advancement

ACUTA Annual Conference & Exhibition

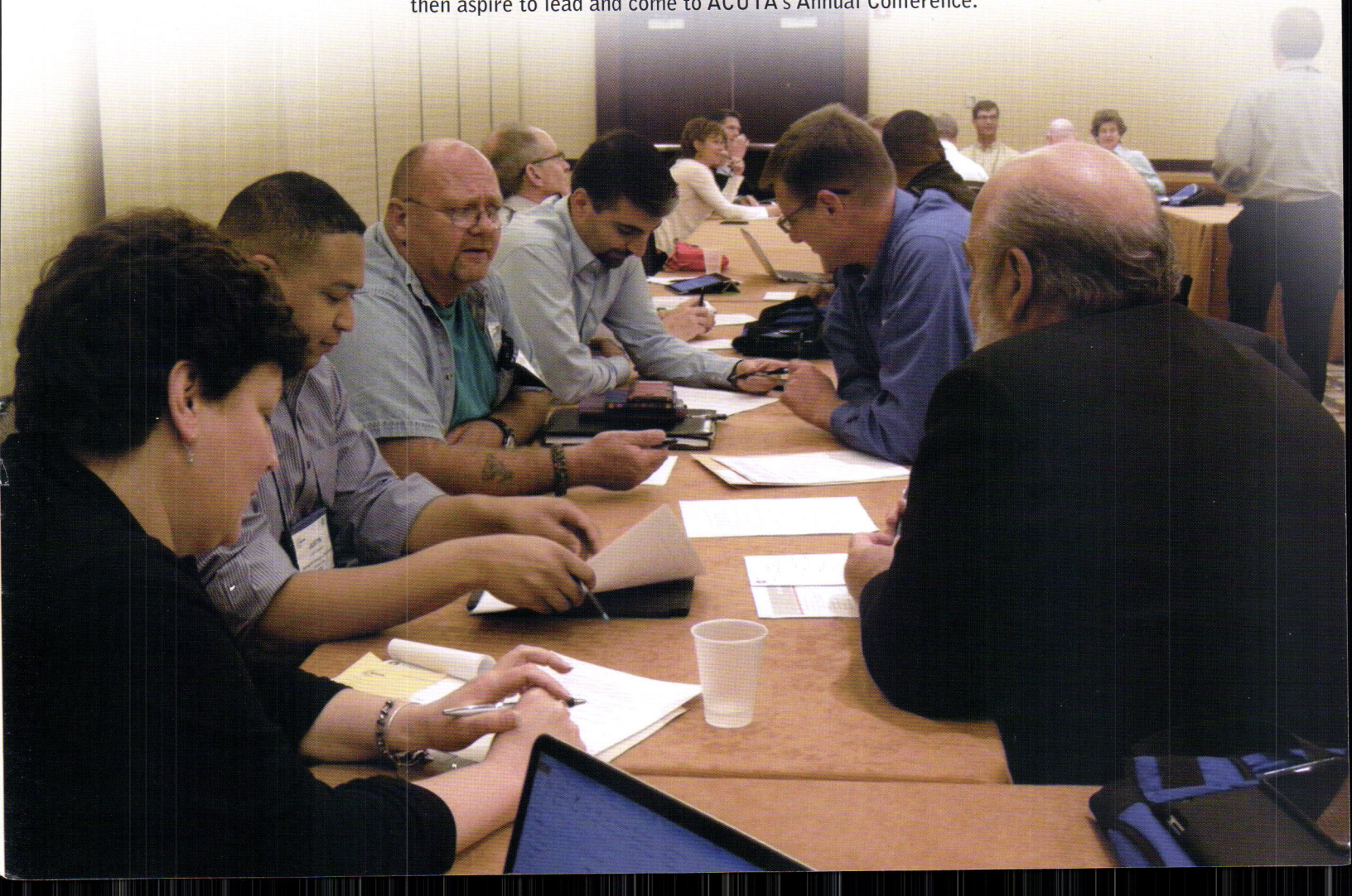
Atlanta, Georgia — April 19-22, 2015

DELIVER
ENGAGE
LEARN
ADVANCE

Leaders are not born, they are forged by experience, challenges and opportunities. Your time to lead is here as campus administrators increasingly look to you for strategies and recommendations that shape multi-million dollar investments. They look to you to solve problems when there is no manual to turn to. In fact, when you do your best work, few notice; things just – work.

From **April 19 – 22, 2015**, technology leaders will meet in **Atlanta for ACUTA's 44th Annual Conference and Exhibition**. Professionals just like you will share the latest information and their experiences, review the leading-edge technologies and services, and discuss the best ideas for confronting tomorrow's challenges. You will be writing the manuals for your own progress.

If you want to be part of shaping the future of campus technologies, if you want to meet and be inspired by your peers, if you have a vision for your campus that you want to share, then aspire to lead and come to ACUTA's Annual Conference.



TALKAPHONE

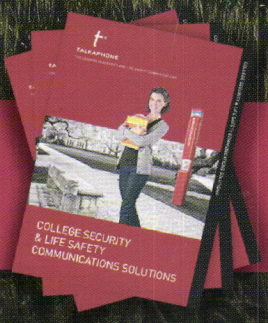
OUR PRODUCTS STAND UP TO THE ELEMENTS.

OUR SUPPORT STANDS OUT FROM THE CROWD.

ONLY TALKAPHONE PROVIDES THE DEDICATED SUPPORT YOU NEED FOR VIRTUALLY ANY SITUATION — STANDARD.

"We test the units periodically, and we never have problems. I've seen other competitors' units fail after one or two storms. These Talkaphone towers have been working without problems for six years strong."

— Don Gussler, Emeryville Marina Harbor Master



Download our College Security & Life Safety Communications Solutions brochure at **www.talkaphone.com/AC45** today.

cisco Compatible

TALKAPHONE'S VoIP-500 SERIES PHONE has tested compatible with Cisco UCM 7.1 and UCM 8.6. Go to www.cisco.com/go/compatibledisclaimer for complete disclaimer.

TALKAPHONE PROUDLY PARTNERS WITH:

OnSSI · singlewire software · MIR3 · Rave MOBILE SAFETY · comnet · FLUIDMESH NETWORKS · milestone · ifs · exacq Technologies