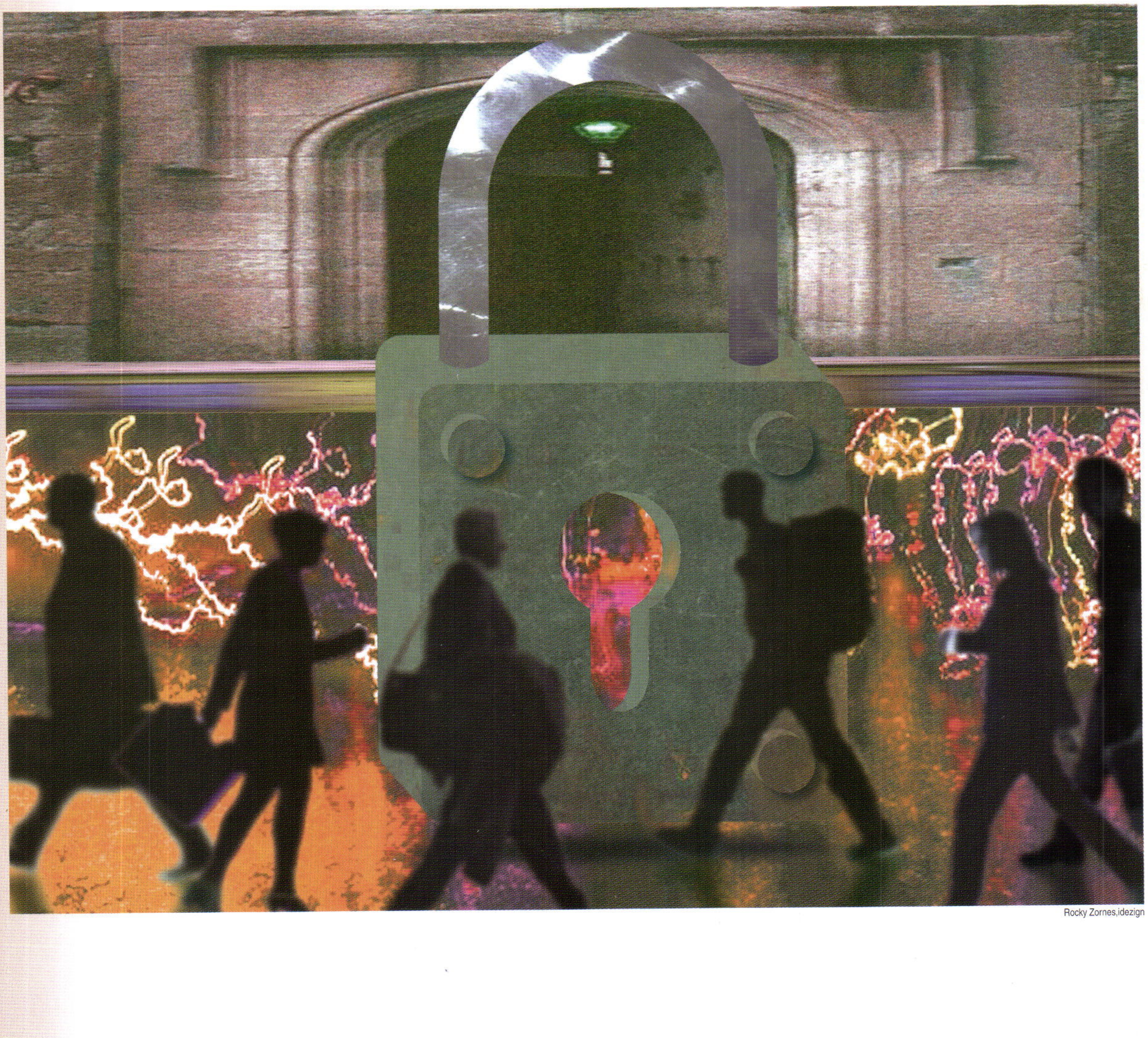
Summer 2006

ACUTA Journal of Telecommunications in Higher Education

Summer, 2006
Vol.10, No.2

ACUTA Journal of Communications Technology in Higher Education

Published by The Association for Communications Technology Professionals in Higher Education



Rocky Zornes,idezign

This Issue: Meeting the Security Challenge

Intelligent PoE

From the most trusted name in power.

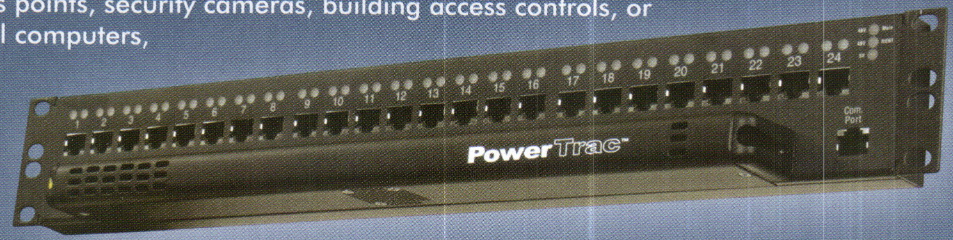
Hubbell PowerTRAC™. Power Over Ethernet.

Today's most intelligent approach to delivering PoE with capabilities to track and manage critical assets.

PowerTRAC™ is a Midspan panel solution that saves valuable closet space and its modular design allows you to select the configurations that meet your requirements.

Whether it's delivering PoE for access points, security cameras, building access controls, or tracking valuable assets like personal computers, **PowerTRAC**™ delivers.

- *Full power to every port.*
- *Reliability and security.*
- *Business critical applications that work.*
- *Rock solid asset management.*
- *Lower cost of ownership.*



- Voice over IP
- Asset Management
- Wireless and Wireless Devices
- Security Systems IP Cameras
- Building Automation/ HVAC Control Systems
- Life Safety Control

HUBBELL®
Hubbell Premise Wiring

14 Lord's Hill Road
Stonington, CT 06378
Tel: (860) 535-8326; 1-800-626-0005
Fax: (860) 535-8328
Internet: www.hubbell-premise.com

Events Calendar

Event	Date	Place
Annual Conference	July 23–27, 2006	Manchester Grand Hyatt San Diego, California
Fall Seminars	October 22–25, 2006	Marriott Portland Downtown Portland,Oregon
Winter Seminars	January 21–24, 2007	Hilton Austin Austin, Texas
Spring Seminars	April 1–4, 2007	Baltimore Marriott Waterfront Hotel Baltimore, Maryland

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

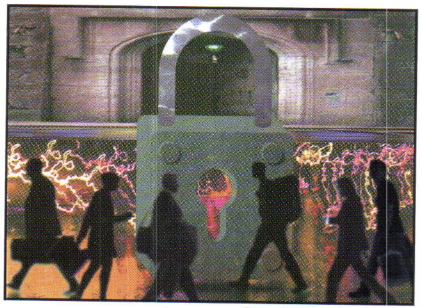
ACUTA's Core Values are:

- Encouraging and facilitating networking and the sharing of resources
- Exhibiting respect for the expression of individual opinions and solutions
- Fulfilling a commitment to professional development and growth
- Advancing the value of communications technologies in higher education
- Encouraging volunteerism and individual contribution of members

Contents

Summer 2006 • Volume 10 Number 2
Meeting the Security Challenge

FEATURES



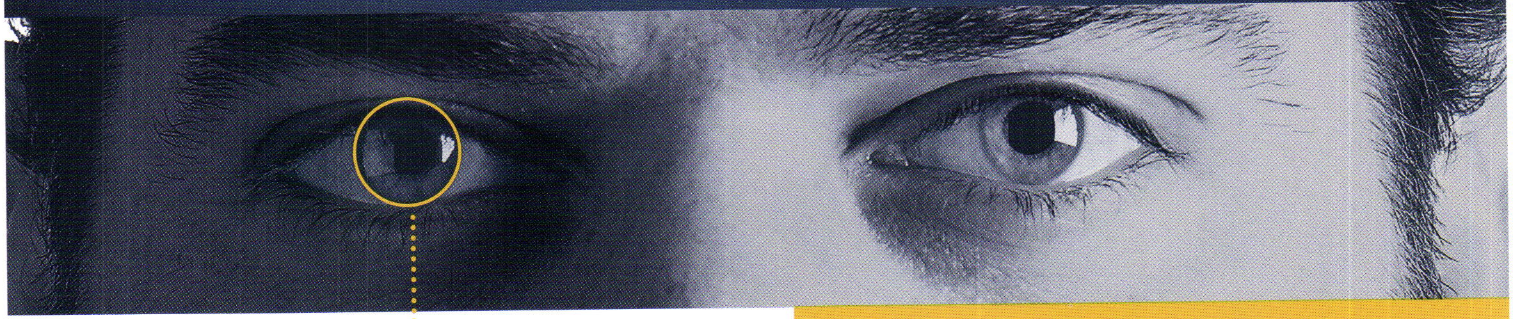
Cover art by Rocky Zornes, idezign

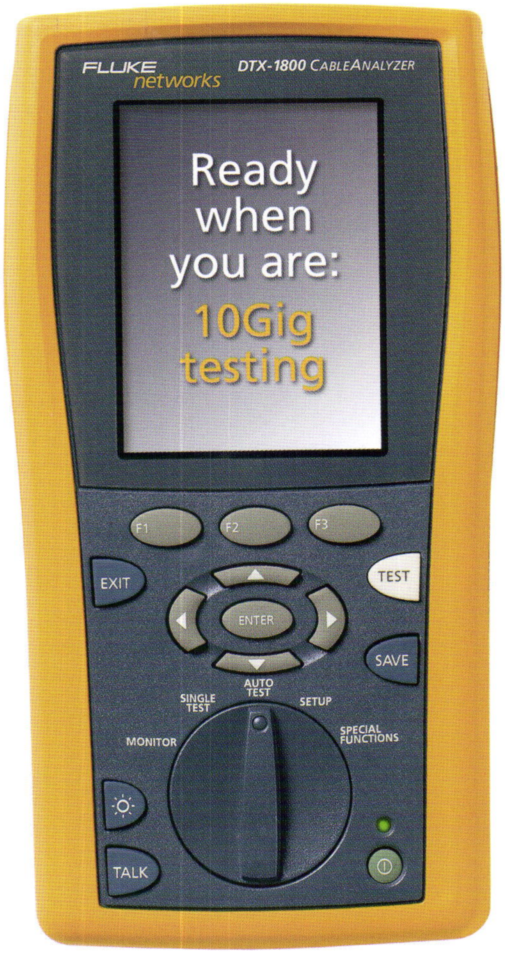
INTERVIEW

COLUMNS

ADVERTISERS' INDEX

See how far the right tool can take you - from 10Meg to 10Gig.





The industry's most powerful cable tester gives you everything you need to put 10Gig to the test—with the DTX CableAnalyzer from Fluke Networks. We were the first to bring digital technology to cable test and certification. The first to provide a complete Cat 6 solution to reduce your total time to certify by as much as 4 hours a day. Now with DTX, we're the first to deliver a 10Gig solution that equips you to meet both today's test standards and the new 10Gig standards including Alien Crosstalk—in one rugged, reliable tool. Like our DSP platform, which served the market for a decade, DTX is built on our commitment to industry-leading speed, accuracy and ease-of-use. So whether you're installing or upgrading your cabling infrastructure, you've got the total 10Gig testing solution at hand. Only from Fluke Networks—the technology leader in network testing. To learn more about 10Gig testing, go to www.flukenetworks.com/campusnetworks and download our whitepaper, "Testing Challenges for 10 Gb/s Ethernet over Copper Cabling."

See how far DTX can take you: check out our DTX 10Gig Solution at the ACUTA Conference booth 607/609. And attend our presentation on Deploying 10GBASE-T Cabling. See the ACUTA Conference Daily for the presentation time and location.

FLUKE networks®

NETWORKSUPERVISION™

> “With an expanding service base and a growing need for unfettered access, it has never been more challenging to protect mission-critical data, applications, services, and campus networks from internal as well as external threats.
>
> *James S. Cross, PhD*
> *Michigan Technological University*
> *page 10*

The ACUTA Journal of Communications Technology in Higher Education

Published Quarterly by
ACUTA: The Association for Communications
Technology Professionals in Higher Education
152 W. Zandale Drive, Suite 200
Lexington, KY 40503-2486

Phone	859/278-3338
Fax	859/278-3268
E-mail	pscott@acuta.org

Publisher
Jeri A. Semer, CAE, Executive Director

Editor-in-Chief
Pat Scott, Communications Manager

Contributing Editor
Curt Harler

Advertising Sales
Amy Burton, Manager, Corp. Relations and Marketing
859/278-3338 or e-mail: aburton@acuta.org

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 upon 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.

ISSN 1097-8658

Postmaster, send all address changes to:

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

Visit the ACUTA site on the World Wide Web:

http://www.acuta.org

Membership and Subscriptions

Subscriptions are provided as a benefit of membership. The publication is available to nonmembers for $80 per year or $20 per issue. For information, contact Kellie Bowman, Membership Development Manager, 859/278-3338, ext. 222, or e-mail kbowman@acuta.org.

Don't Make a Million Dollar Voice Messaging Mistake

How much money can you expect to spend if you change to a new family of messaging systems? Our customers tell us that it's twice as expensive to purchase a new messaging system versus upgrading their current system!

Why?

- There is a huge time and expense commitment in training new users, re-recording greetings and auto attendants and rebuilding distribution lists.
- Users resist learning new user interfaces, and get little help from confused employees and overwhelmed help desks.
- Database conversions can be more complicated than anticipated.

At **CommuniTech Services**, we've specialized in providing and supporting voice messaging systems since 1983. We have the answers that solve your most critical concerns, including these:

Have you made sure that that the critical features you use now are available on your new system?
New "state-of-the-art" systems often lack the features you expect. Some don't even offer automated attendant.

Does your vendor know both the voice messaging applications and the capabilities of the new technology and can bridge the old with the new?
We know messaging intimately in both the TDM and IP worlds along with *Find Me, Follow Me, Unified Messaging, IVR,* and *Speech Recognition* and other productivity enhancers. Don't pay for your vendor's learning curve.

Does your vendor know how to proactively monitor and optimize systems that have heavy demand, high up-time requirements?
This is part of our standard support service. Don't wait for your system to malfunction...we'll make sure it never does.

If you're considering a messaging product from your PBX vendor, is their experience limited to just integrating their own messaging system to their own phone system? What if you need to integrate with other PBX's, e-mail or Presence servers, Speech Recognition, IVR or other Voice Messaging platforms?
As a messaging focused systems integrator, we can handle all of your future needs.

Does your system have the latest design considerations for up-time and high security requirements?
Our systems are built for maximum reliability and up-time. From the operating system to the CPU and power supplies, we are focused on insuring your up-time.

Can your vendor help devise marketing programs to help you get your user communities to use your services and to help you sell your services?
We'll help you sell your users on the services you provide (and offer special revenue generating programs that target students.)

What other hidden costs of ownership are there?
Many vendors are inexperienced in sizing systems which leads to spending more than is necessary. We'll help you make the right decision the first time. Needs change – an expert in messaging can ensure that your messaging platform can adapt and thrive in an ever changing, complex environment.

CommuniTech Services can help you avoid potentially costly mistakes with your messaging systems needs. For more information, call us at 847.981.1200 extension 480.

CS

COMMUNITECH SERVICES, INC.

www.communitechservices.com

PRESIDENT'S MESSAGE

Patricia A. Todus
Northwestern University
ACUTA President
2005–2006

Meeting the Security Challenge

It is truly amazing the new heights of visibility that security and all its corresponding issues have attained in our institutions. Thinking back before 9/11, we all focused our energies on Y2K efforts to make sure that our information was safe and our systems were protected or backed up in case of a catastrophic event. For reasons too numerous to mention, Y2K was a nonevent. It did, for many of us, raise our awareness of the need for disaster recovery, business continuity practices, and security.

Following the unbelievable events of 9/11, the United States government, businesses, educational institutions, and people everywhere began to plan and implement security measures to protect themselves from everything from loss of information to loss of life.

In the world of higher education, academic freedom and research creativity are a given. When these are combined in our environment with the dramatic growth in electronic business processes, the increase in information flow internally and externally, and the introduction of new, possibly disruptive technologies, there are unique security and compliance challenges. Many of us now have security offices with chief security officers. This office reviews and remediates security events occurring inside and outside the university environment, develops plans to proactively address security requirements, and is actively involved in and focused on security measures and compliance regulations introduced by our government.

All of this equates to increasing the level of awareness on our campuses. This is an ongoing marketing campaign, representing a collaborative effort of our administrative leaders, researchers, faculty, staff, and students. The combination of intelligent security direction and collaboration, fostered in university environments, has allowed universities to respond to the increasing demands of attaining the level of security and compliance necessary in this new world in which we live.

The demands on resources needed to continue this effort will grow exponentially. Because of the pressure on resources and the need for more of them, it is important to address security and compliance issues in an efficient and thoughtful manner. Security and compliance in higher education are a never-ending challenge for our community. Our institutions may never have the resources necessary to obliterate all security issues and address completely all compliance measures. We will, as we have before, address them using our strengths of collaboration and creativity.

Organizations such as ACUTA play a very important role in this new world, providing both education about security-related issues and a forum in which members share ideas and information that further improve security and compliance on our campuses. In addition, ACUTA has established and maintains a higher-education presence in Washington as our government considers regulations and compliance measures. Working together we are better prepared to protect ourselves and our constituencies against the challenges sure to come.

▼

Best Practices in IT/Telecom Management Software for Colleges and Universities

COMPCO

2006

Compco Customer Relationships

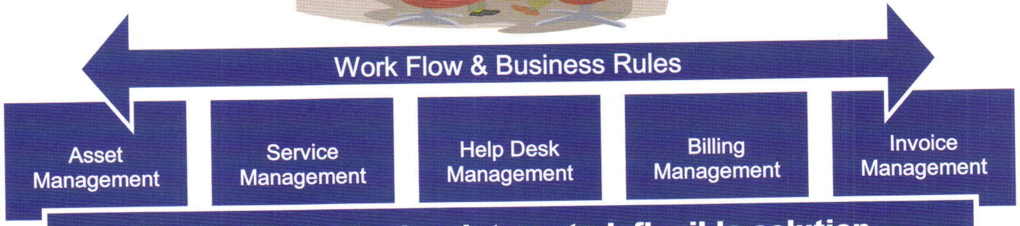
COLLEGES & UNIVERSITIES

75

IN THE FOLLOWING STATES:

Alabama
California
Connecticut
Florida
Georgia
Iowa
Illinois
Indiana
Kansas
Kentucky
Louisiana
Maine
Maryland
Massachusetts
Michigan
Minnesota
Mississippi
Missouri
North Carolina
Nebraska
New Jersey
Ohio
Pennsylvania
South Carolina
Tennessee
Texas
Virginia
Wisconsin
West Virginia
and 2 Canadian provinces

What is Your University's Goal for Total Technology Management Software?



Work Flow & Business Rules

Asset Management

Service Management

Help Desk Management

Billing Management

Invoice Management

One comprehensive, integrated, flexible solution that delivers total system-wide accountability, visibility, control and access.

Your Goals Can Be Realized with Compco Software

Twenty-eight years of experience in management software combined with input from great customers in college/university, healthcare, government, and corporate environments help turn your goals into realities. Compco's MySoft.net with Mpower Technology gives you the:

- FREEDOM TO INNOVATE
- FLEXIBILITY TO CUSTOMIZE
- POWER TO EXECUTE

> "We evaluated the major software vendors and found that Compco's MySoft.net software is, by far, the best for managing voice and data networks."
>
> Angela Bradley, Director of Telecom, Iowa State University

(615) 373-3636 ext. 148 rburns@compco.com www.compco.com

From the Executive Director

Innovations Converge Security and IT

Jeri A. Semer, CAE
ACUTA Executive Director

Colleges and universities are typically ahead of the curve in the adoption of innovative technologies. Perhaps that is due to a combination of the research-focused culture of higher education and the communications and networking demands of a unique population.

It was true back when the network meant the telephone system, and it is true today with the convergence of data, voice, and video systems. With user populations ranging from campus administrative departments to instructors leading distance education courses, and from students doing peer-to-peer file sharing to researchers moving gigabytes of data back and forth daily, the higher education campus is a true test bed for effective network architectures.

In my opinion, that is one of the reasons that ACUTA exists. Our organization, representing more than 800 institutions and 135 corporations, is dedicated to supporting members in their ability to leverage technology to contribute to the strategic missions of their institutions. We occupy a unique position as a clearinghouse of information about the technological initiatives and successes of colleges and universities.

This innovation extends to the sensitive issue of campus security. The need to keep students, employees, and visitors safe and to protect the physical and intellectual assets of the university is a truly real-time need. Many ACUTA members are leading the way in enabling campus security using the high-speed, high-capacity networks that they use to handle voice and data.

Earlier this year, I learned about these efforts at several member institutions. I thought they would offer interesting examples of how the worlds of physical security and technology are converging on campus, and how ACUTA members are working closely with campus security officials to enhance security and safety.

Louisiana State University, Bridgewater State College, and Providence College are diverse in geography, size, and environment, but they all have one important thing in common—a willingness to innovate to converge security and IT.

Louisiana State University in Baton Rouge has been using its data network to transport security video images and operations monitoring data in the nearly two years since the 30,000-student school moved to a routed 10-gigabit Ethernet network.

LSU has two sources for its security video. For general campus security, there are about 18 cameras, whose locations were determined by campus security personnel. They cover nearly all of the campus, and their video streams feed to a central site for monitoring. Separately, the veterinary school has its own camera system, which is closely monitored because some of the research done there falls under the purview of the U. S. Department of Homeland Security. All the camera traffic runs over gigabit interfaces. A private VLAN prevents the security video from being seen on public VLANs when it goes to the server to be written to disk.

In addition, the network provides transport for data from fire, environmental, and security alarms and building access systems. The IT department provides network transport for the data but does not get involved with the monitoring. We were told that LSU plans to expand its network of cameras and can expand substantially without straining network capacity.

Bridgewater State College in Massachusetts monitors the security of classroom audio-visual equipment as well as buildings over its data network. The IT department at the 9,300-student college is just completing a major upgrade to the network. Bridgewater has a gigabit Ethernet backbone network with 100 megabits-per-second links to each desktop.

Bridgewater recently completed a classroom technology project in 41 general purpose classrooms. They installed projectors, computers, document cameras, DVD players, and control systems. They also created a monitoring station in their support area, and if any of those classroom devices is disconnected, an alarm goes off.

The monitoring uses Simple Network Management Protocol (SNMP) to constantly send messages to the classroom equipment. If at any time a piece of equipment doesn't answer its call, that indicates that it has most likely been disconnected. The monitoring data goes to campus security and to the IT department simultaneously. The next phase of the project will involve the second-tier classrooms, and as each classroom receives an equipment upgrade, that equipment will be linked to the central monitoring system.

Building-access information at Bridgewater is also carried over the data network for monitoring by campus security, utilizing sensors on every door. In addition, nearly all of the telecommunications network wiring closets, as well as the main computer and switch rooms, are now monitored via the network.

At **Providence College** in Rhode Island, an 89-year-old college with 4,800 students, full-motion security video surveillance data is now streamed over the main campus network. The college recently upgraded its system with new cameras and large plasma screens. The camera traffic has been moved from the cable television fiber system to the main campus data network in order to meet current and future needs, including an eventual transition to IP cameras.

Some two dozen cameras are in place, covering approximately half of the Providence campus. Their locations were determined by the school's director of security and safety. Installing the cameras and connecting them to the network is a joint effort of the public safety and IT departments. A campus representative told us that, although there is not much crime on campus, they have spotted a few property vandalism incidents. More importantly, the project has created awareness that there is increased video surveillance.

At Providence, the main campus network also transmits building access data. Every dormitory and campus apartment requires card access, as does a bar on campus and, of course, all "sensitive" rooms, such as those housing computer and telephony equipment.

As the successful applications of merged physical security and IT at these three ACUTA member institutions (and many more) demonstrate, there are clear benefits to this aspect of convergence. It is a trend that we see likely to continue, and a clear indication of how communications technology is enhancing and safeguarding the quality of life on campus.

▼

Network Security: An Achilles Heel for Organizations of All Sizes

"Whoever is first in the field and awaits the coming of the enemy will be fresh for the fight."
— Sun Tzu

by James S. Cross, PhD

It seems they are everywhere: threats, security breaches, crackers, and hackers attempting to break into networks to steal, destroy, and launch malware. With an expanding service base and a growing need for unfettered access, it has never been more challenging to protect mission-critical data, applications, services, and campus networks from internal as well as external threats.

Some computer experts have dubbed 2005 the "worst year ever" for known computer security breaches. According to Gary Bloom, vice chairman and president of Symantec, "It's a new frontier for security. Just protecting the endpoint from malware or monitoring the wire is not nearly enough....The world has moved on and become more subtle, interconnected, and dangerous. The world has transitioned from disruptive attacks to outright fraud; moved from prevention of malicious code execution to surveillance, monitoring, and prevention of any malicious activity, all in a regulated society."[1] Security risks, threat potentials, and the necessity to find ways to tackle them have never been greater.

According to Jessica Rivchin in "Security Breaches Continue," measuring the actual number of break-ins is difficult, since many companies are unaware that they have been hacked.[2] Many security experts say there is little doubt that there are more digital attacks to come because of the rapid commoditization of the Internet and the consumer-security market. The Internet has long been a major security concern for many industries worldwide, from the corporate spheres to various government departments. It is not just about blocking incoming traffic and who connects to our enterprise networks. Protecting information and understanding what goes on within an organization's network is just as important. As hackers become increasingly skilled, security professionals will need to work smarter to stay ahead of online threats and beef up their security measures as they integrate new technologies into their enterprise networks.

New Questions: Biometric Answers?

New challenges are being presented by "social computing," "wikis," and "personal broadcasting," as podcasts, weblogs, and video blogs continue to emerge as a big technology area. Designed to support collaborative environments, social computing and personal broadcasting contribute to what experts see as a plethora of challenges for colleges' and universities' protection schemes, such as:

- ID management
- network access control
- adaptive threat defense
- bandwidth management
- open policy-based culture
- security policy enforcement

ID management and network access controls to detect, isolate, and clean infected and/or vulnerable wired and wireless devices attempting to access the network are critical functions in maintaining a high-performance network environment. Security-minded network administrators are working to get a better grip on their sprawling information systems, adaptive threat defenses, timely identification and mitigation of security threats, and bandwidth management to share available capacity more equitably and effectively.[3]

To that end, many have adopted a wide array of network access controls and adaptive threat defenses. However, many network administrators are finding their current controls and defense strategies are only somewhat effective. The consequences are increased security vulnerabilities, poor network performance, risk of failing compliance audits, unexplained outages, and more unplanned work for staff.

Many organizations are beginning to research and explore biometrics for possible insights into more effective security management. Biometric systems identify would-be users by face, voice, fingerprint, hand geometry, iris, or other physical or behavioral characteristics. While still not foolproof, such systems represent an improvement over traditional methods such as passwords or ID cards.[4]

Perhaps the biggest obstacle to implementing biometrics is people. Privacy issues, of heightened concern to Americans in the wake of 9/11 and the war on terrorism, raise concern about the potential for misuse, abuse, or even criminal activity. But the benefits of enhanced security seem to be outweighing the risk of intrusion into our private lives.

New Products Stepping Up Security

According to Robert Guth of the *Wall Street Journal,* six of America's largest financial institutions are taking a "strength in numbers" approach to guard sensitive data, applications, and services.[5] The six banks (Bank of America, Bank of New York, Citigroup, JP Morgan Chase, Wells Fargo, and US Bancorp), backed by the Washington Financial Services Roundtable financial services industry group, and some major accounting firms are adopting common guidelines that their suppliers and partners will have to follow. The program is designed to raise

▶

Consulting In Information Technology, Telecommunications, and Networks In Higher Education
WTC
Strategy
Acquisition
Since 1983
Implementation
213-622-4444
www.wtc-inc.net
wtc@wtc-inc.net

the bar on security across the industry and formalize security procedures that have been largely ad hoc. Catherine Allen, of the Washington Financial Services Roundtable industry group, states, "We're trying to create a standardized approach and a much more rigorous approach" to security in response to scrutiny of how financial institutions handle and protect sensitive data.[6]

The rash of identity thefts has businesses, government agencies, and higher education institutions exploring new options for locking down resources and implementing new tools to control access and security. The costs, time, and complexities of managing security systems can be an Achilles heel for organizations of all sizes. According to Rich Mogull, a Gartner analyst, data-monitoring products that aid in foiling data theft are not in widespread use.[7] Pete Lindstrom, a Spire Security analyst, states, "Detecting when an authorized user is accessing data for fraudulent purposes is difficult."[8]

Although vendors cannot guarantee that their products will detect all occurrences of data theft, products from companies such as SecureWave, Ambeo, Guardium, Lumigent, IPLocks, Verdasys, and Application Security can help by watching databases and servers for content misuse. Other vendors such as Vonu, Tablus, Vericept, Reconnex, and Vidius have developed gateway-style products that watch for sensitive data being accessed, retrieved, and transmitted. While various products can help in foiling security breaches, the problem is unlikely to be solved through technology alone. Mogull of Gartner states, "We need to change the system, and there needs to be a long look at finding alternative methods."[9]

To that end, Permeo Technologies, Checkpoint, Aventail, Juniper, and Sygate have developed products that scan computers as they try to access databases from remote VPN locations and check to see if they have properly patched and updated OSs, antivirus software, and firewalls. The software continues to monitor the computer throughout the session for compliance by "white listing" applications and data that the remote computer cannot access. These products can aid in effectively blocking malware and other nonmalicious applications such as Kazaa, Ares, and Limewire that organizations may not want executed during a remote VPN session.

Security Breaches in High Places

According to "A Chronology of Data Breaches Reported Since the ChoicePoint Incident," more than 50 security breaches were reported by colleges and universities from February to December 2005.[10] The mix of institutions reporting ranged from two-year to research doctoral. The security breaches were reported because they involved personal information useful in identity theft such as Social Security numbers, account numbers, cancelled checks, credit card numbers, and driver's license numbers. The catalyst for reporting the security breaches was the California law enacted in July 2003 that required notice of security breaches involving personal information. Read details on this law at the following websites:
(1) www.privacyrights.org/ar/SecurityBreach.htm
(2) www.privacy.ca.gov/recommendations/secbreach.pdf

The chronology begins February 15, 2005, when data-collection company ChoicePoint made headlines with its announcement of a security breach that affected more than 140,000 people in all 50 states and more than 800 cases of identity theft. This announcement was a watershed event in disclosure to affected individuals. The chronology states, "Since then, the 'best practice' has been to disclose breaches to individuals nationwide—in a sense, adopting California's notice requirement nationally."[11] The database giant will pay $15 million in fines and other penalties, according to the Federal Trade Commission, after disclosing the security breach set off a national debate. The $15 million fine was the largest civil fine in FTC history. In finalizing a settlement with the FTC, the company agreed to set up a fund to aid victims harmed by the breach.[12] ChoicePoint will also have to implement new security measures and have an independent auditor review its security system until 2026.

Ari Schwartz, associate director at CDT states, "There certainly is agreement that we need better notification, exactly because of cases like this. We're seeing data companies selling it to a lot of different people.[13]

More than half the states and the U.S. Congress are considering legislation in which security breach notices would be mandated nationwide. For a list of those states enacting or considering security breach and freeze laws, visit the following Consumers Union websites:

- Security breach notice laws: www.consumersunion.org/campaigns/Breach_laws_May05.pdf
- Security freeze laws: www.consumersunion.org/campaigns/learn_more/002355indiv.html
- State security freeze bills pending in 2006: www.financialprivacynow.org

The following are other sources for security breach information:

- Identity Theft Resource Center: www.idtheftcenter.org/breaches.pdf
- Adam Shostack's blog: www.emergentchaos.com/archives/cat_breaches.html

- Attrition: www.attrition.org/errata/dataloss.html
- World Privacy Forum, Security Breaches in the Digital Medical Environment (scroll to section D of testimony): www.worldprivacyforum.org/testimony/NCVHStestimony_092005.html

Conclusion

Network security continues to be an Achilles heel for organizations of all sizes as cybercrime takes its toll. The revelation of the security breach at ChoicePoint has led to renewed calls in Washington for a national data privacy law. In addition to calls for legislation from privacy groups, Senator Dianne Feinstein has called for a congressional hearing on Feinstein's Notification of Risk to Personal Data Act. The act would require businesses and government agencies to notify victims when there is a reasonable basis to conclude that a criminal has obtained unencrypted personal information.[14]

Derek V. Smith, ChoicePoint chairman and CEO, states, "The events of early 2005 provided critical lessons from which ChoicePoint and, indeed, the entire industry have learned a great deal."[15]

The loss of consumer confidence from repeated security breaches is the largest threat facing the Internet community, according to Symantec Corporation chief executive John Thompson. "If we fail to create a trusted online environment, we'll not only slow the growth of e-commerce, but all business; not just the digital economy, but the whole economy," he said during a keynote speech at the recent RSA Conference.[16] The result is the need for a better solution that organizations can employ in a dynamic environment to spot trends in the threat landscape and be proactive in thwarting modern-day attacks.

A former president of ACUTA, Dr. James Cross is currently a professor of computer and network administration and associate dean of the School of Technology at Michigan Technological University. Reach him at jcross@mtu.edu.

Notes

[1] Illena Armstrong, "2006 RSA Conference," *SC Magazine News,* Feb. 8, 2006.

[2] Jessica Rivchin, "Security Breaches Continue," MobileEnterpriseMag.com, Feb. 1, 2006.

[3] "The Good, the Bad and the Ugly: Cybercrime Take Tool," *Network World,* Jan. 30, 2006, 6.

[4] Andy Dornan, "Biometrics Becomes a Commodity," *IT Architect,* Feb. 2006, 46; David Greenfield, "Automating IT," *IT Architect,* Feb. 2006, 20.

[5] Robert A. Guth, "Banks Begin New Secure-Data Effort," *Wall Street Journal,* Feb. 1, 2006, A8.

[6] Ibid.

[7] Ellen Messmer, "High-Profile Identity Theft Force Govt, Industry To Take Action," *Network World.* Mar. 28, 2005, 1.

[8] Ibid.

[9] Ibid.

[10] Privacy Rights Clearinghouse, "A Chronology of Data Breaches Reported Since the ChoicePoint Incident," posted Apr. 20, 2005, updated Jan. 31, 2006, www.privacyrights.org.

[11] Ibid.

[12] "Newsbits: ChoicePoint to Pay Fine for Breach," *Network World,* Jan. 30, 2006, 6.

[13] Grant Gross, "ChoicePoint's Error Sparks Talk of ID Theft Law," IDG News Service, Feb. 23, 2005.

[14] Ibid.

[15] Grant Gross, "ChoicePoint to Pay $15 Million for Data Breach," IDG News Service. Jan. 26, 2006.

[16] Roger Cheng, "Symantec CEO Says Security Vital to Keep Confidence in Internet," MarketWatch, Feb. 15, 2006.

Additional reading: Cara Garretson, "ID Theft, the Sequel," *Network World,* Jan. 30, 2006, 1.

▼

Providing Backup in a VoIP World

by Curt Harler

Linus had his security blanket. When Snoopy stole it away, Linus's life was turned upside-down.

In the telephony world, communications managers always had a nice, warm feeling knowing that the power to run the phone system would always be there. Students and staff could call for help—even if the campus electric grid failed.

Happiness, to paraphrase Charles Schulz, was a black handset. With the coming of new, computer-based technology, that feeling of happiness based on security is snatched away.

"When nothing else works, we've always relied on the phone," said Larry Maughan, director of ITS/communications at Salt Lake Community College, Salt Lake City, Utah. "Sad to say, VoIP without adequate power backup certainly fails the test.

"Think about the times at our homes we've lost power and been sitting in the dark. It's a comforting thought to know (provided you don't exclusively use cordless phones) that you can at least call the power company to report the outage or talk to friends," Maughan said.

"For me there is a certain comfort and confidence associated with dialtone," Maughan continues. "In my mind, there will always be—until the power and reliability issues are dealt with—a concern about VoIP, POE, UPS, and so on."

Theresa Rowe, assistant vice president for university technology services at Oakland University, Rochester, Michigan, said her team considered a number of points when the group was discussing plans for VoIP. Some of the options were technically oriented, others were service oriented. Some are making service changes:

1. Phone drop but no phone
2. No service at all
3. Campus-only service (house phones)

Others are keeping services, but making technical changes, and there are options:

1. VoIP with a "reslife" phone assignment such as Cisco 7940 phones
2. SIP phones
3. Analog voice gateways
4. Keeping the PBX active for the residence halls.

Table 1. VoIP wiring closet heat output calculation worksheet

ITEM	DATA REQUIRED	HEAT OUTPUT CALCULATION	HEAT OUTPUT SUBTOTAL
Switches without in-line power, other IT equipment (except midspan power units)	Sum of input-rated power in watts	Same as total IT load power in watts	______ watts
Switch with in-line power capability	Input rated power in watts	0.6 x input power rating	______ watts
Midspan power units	Input rated power in watts	0.4 x input power rating	______ watts
Lighting	Power rating of any lighting devices permanently on in watts	Power rating	______ watts
UPS system	Power rating of the UPS system (not the load) in watts	0.09 x UPS power rating	______ watts
Total	Subtotals from above	Sum of the above heat output subtotals	______ watts

©American Power Conversion. Used with permission.

VoIP Growing Fast

There is no question that VoIP is growing like kudzu. According to the Telecommunications Industry Association's 2006 Telecommunications Market Review and Forecast, the number of VoIP customers (not including PC-to-PC services) more than tripled, to 4.2 million, in 2005.

TIA said that figure is expected to grow by a compound annual rate of 43.9 percent through 2009, when it will reach 18.0 million. This comes on the heels of an eightfold increase from 150,000 at the end of 2003 to 1.2 million at the end of 2004. For the university community, the growth of VoIP means playing an old game with an entirely new set of rules.

Brian Buckler, director of network and telecommunications operations at the University of California, Irvine, faced the usual trade-offs between desires and dollars.

"For us at UCI it is a question of what is ideal versus what is affordable," Buckler said. Interestingly, desire won out in one case he managed, and dollars won in the other.

"We have two newly constructed buildings with production Cisco VoIP, and one is ideal and one is affordable," Buckler said.

"In the ideal building, we have Cisco 6500s providing GE POE to every jack (to be used for voice or data), and each 6500 is connected to a centralized 40KVA UPS that is connected to the building generator. We also have red emergency wall phones in the hallways connected to our Ericsson MD110 PBX analog ports.

"In the 'affordable' building," Buckler continues, "we provide one 24-port 100MB POE switch per floor to support IP phones, and only these POE switches and their distribution switches dedicated to voice are connected to a centralized 15KVA UPS connected to the building generator."

Telecommunications closets at Suffolk County Community College in Selden, New York, have been upgraded to three hours' UPS backup for all VoIP switches, said Rich Johnson, director of networks and telecom. The primary servers and analog gateways have generator backup.

"We also use the APS InfrStructure appliance with temperature/humidity sensors in all 75 wire closets," Johnson said.

Backup and heat management are keys to a successful VoIP deployment. (See Table 1 for VoIP wiring closet heat output calculation worksheet.)

One Step or Four

"There is no clear answer or guiding standard here," said Viswas Purani, director, emerging technologies and applications at American Power Conversion Corporation, (www.apcc.com, East Providence, Rhode Island). "With regard to battery backup for VoIP, we have seen from one hour to four or even eight hours."

In legacy telephony, the central office provides power that can range from eight hours to 24 hours. "Business process availability and 911 are the two most obvious concerns here," he said.

▶

Purani said he feels the best approach to UPS for VoIP phones is to do Power over Ethernet (PoE) per the IEEE 802.3af standard. "That way, you don't have hundreds of UPSs spread out across a campus which you have to buy, install, manage, and maintain," he explained. "Needless to say, that is expensive."

On a small campus, or for a standalone application with fewer than 100 users, the VoIP server and switch will typically be in one box. In that case, PoE is the way to go.

At a bigger campus, he recommends taking a four-step approach, handling the desktop, the integrated distribution frame (IDF), the main distribution frame (MDF), and the call-routing servers as separate situations.

At the desktop, where the handset resides, PoE works. "What we have seen is people typically go with one hour's worth of battery backup," Purani said. "It can be more or less depending upon your budget and comfort levels."

At the closet, the midspan power patch panel, between the phone and the switch, will take in Ethernet on one plug and PoE at the other side. On newer switches (those less than two years old), that power feature usually is built in. Otherwise, provide a UPS for the closet.

"By doing PoE, just one UPS in the closet (two if you want redundancy) supports the switches/routers in the closet as well as providing battery backup power to the phones. This is much simpler, cleaner, and more cost effective," he continues.

He recommends that a closet handle between 10 and 500 users. The backup power requirement is 15 watts per port. So, a building with 100 ports would require 1,500 watts.

All new phones are PoE capable, complying with IEEE 802.3af. "If there are old VoIP phones which have to be plugged into the wall, then you will need a UPS for riding through a power outage," Purani added.

From the IDF, lines go to the MDF for demarcation. This gateway to the Internet and backhaul should have chassis-based switches, which need to be protected according to the manufacturer's specifications.

The last piece is the servers that route calls and provide CLASS features and functionality. These typically are in a data center and should be given serious backup time.

Purani sums up the four-level hierarchy: in the closet, provide one hour's protection unless the phones provide a vital safety function; at the core MDF, two to four hours is sufficient; at the servers, four to eight hours is required. Of course, that can vary with an administrator's comfort levels.

Reviewing the Listserv

The ACUTA listserv was quite active on the topic. Oakland University's Rowe did a good job of summarizing the comments made.

Phone service should match building occupancy expectations, considering local inspection rules for emergency lighting and the purpose of the operation in the building, she said. Rowe shares Purani's belief that a health center or police department, with 24-hour, seven-day occupancy expectations, even through power outages, will require more backup power planning for emergencies than a standard classroom.

"Most of us are giving special considerations to planning out VoIP for residential living areas; decisions made for lifestyle may not match the other areas of campus," Rowe said.

The run time from the UPS likely will correspond to the expected time of occupancy of the building. A common minimum is 30 minutes runtime at five years of battery life in every closet that had VoIP POE switches. Some are planning for up to two hours, which seems to be the outside range.

Network closets should be supported by a single UPS in the building for best management practice, planning for routine maintenance and battery replacement. At the least, UPS is needed in every closet.

Generators are not generally viewed as a necessity, but if the campus is planning an emergency power grid, consideration of the phones should be included.

Georgia State University is installing UPSs in all telecom closets. All will have 30-minute or greater ratings.

"Our central communications manager/call processing servers will be located in the Network Operation Center (NOC)," said Georgia State's Mark Roberson. The NOC is serviced by UPS and a flywheel generator. But it does not stop there. In addition, 10 to 15 of the other buildings at Georgia State are on a generator.

Roberson's feeling is that, with the ubiquity of cellular phones, 30 minutes of power after a building is dark should be plenty for contacting emergency crews and the like.

"However, like other universities, we face 'no power/no work'!" he said. In a crunch, students, faculty, and staff are not allowed to remain in the administrative buildings because of life-safety issues. Residence halls are handled differently.

The residence halls were outsourced, but the provider is offering a hybrid VoIP upgrade solution. In Georgia State's case, the Housing Office pays for one analog dialtone to each suite.

"Students wanting a private phone have the option of purchasing the service directly from a service provider. That offering is VoIP, Roberson explained. There are UPSs in each data closet to support the data/voice network.

"All network ports in administrative areas are PoE. We only install non-PoE switches in spaces dedicated for computer labs," Roberson said.

They maintain several Centrex lines in each building for backup. "I've also recommended keeping all elevators and alarm lines on Centrex," he added.

At UC Irvine, the network backbone is on UPS and a generator.

"To retrofit old buildings with IP phones, we may need to cut even more corners to make it affordable," Buckler said. "At a minimum, the IP phone ports will be on POE switches connected to UPS systems.

"Our preference is to put in a centralized UPS in each building to support all the POE switches and the distribution switches (and ideally all of the network equipment) rather than a UPS in each communications equipment room. We believe that a centralized UPS approach is more manageable and offers longer battery life," Buckler said.

In a perfect world, he said he would like to be able to afford more than 30 minutes of backup time. "I'd rather see closer to two hours," he said, adding that UPS battery time is not an issue if a college has a generator with an automatic transfer switch.

"I just don't know if it will be affordable to put a generator and centralized UPS in each building, and to build the electrical distribution infrastructure from the UPS to each equipment room," he said. "We are currently estimating those costs for our campus with about 200 buildings."

Maughan said he favors the idea of a hybrid system. "I can run VoIP where I need it and it makes sense, and utilize my digital voice network in the areas where I have a perfectly reliable cabled network with generator backup.

He admits that his is a conservative approach. "It allows me to utilize a blend of technologies for the good of the college and leverage my existing platform," he explained.

Brandeis University has a Cisco Emergency Responder (CER). The system knows the location of every switch port on campus, so when a 911 call comes in, it automatically sends the location information—regardless of what phone is plugged in.

John Turner, associate director for networks and systems, said they have an ERL per floor on most of their buildings. "But we cheat a bit because we don't send our 911 calls to an off-site PSAP. Our calls are sent to our local campus police office," he said. Campus police have the CER software on their PCs. When a call comes in, it identifies the caller's location down to the room and jack.

"CER is a great product. We only use about 60 percent of it," Turner said. He maintains that CER is, unfortunately, a very misunderstood application. "No one in our region really understands it," he said. Yet, he is optimistic about the utility of CER. "I spoke with the principal developers of Call Manager and CER at a users group, and they expressed interest in making some dramatic improvements over the next few releases," Turner added.

"We're not there yet, but colleagues I've talked to seem to feel that having UPSs in every closet is a necessity, but not generators," shares Joel P. Cooper, director, information technology services at Carleton College, Northfield, Minnesota. He notes that the UPS promises 30 minutes of uptime after a failure and feels that is adequate.

"Costing for this, of course, has to include regular health checks for the UPS units and scheduled battery replacements," Cooper added.

Down the Road

Ron Walczak, principal consultant with Walczak Technology Consultants Inc. (www.walczakconsultants.com, Prospect, Pennsylvania), said that there is a standard now in the finalization process called IEEE 802.1AB Link Layer Discovery Protocol-MED or LLDP-MED which will be the long-term answer to many colleges' problems. He expects the standard to be finalized sometime in the middle to latter portion of 2006.

"Both data switches and phone systems must be compliant—and it will track the phone," he said.

Purani agrees. "A fall-back strategy which is popular is to have some legacy telephone lines in conference rooms and reception areas," he said.

Curt Harler is a contributing editor to the *ACUTA Journal* and a freelance writer who specializes in technology topics. Reach him at curtharler@adelphia.net.

▼

Security Concerns Shift Inward

by Paul Korzeniowski

Once the Internet became popular, communications managers had to lock down their networks and prevent viruses and malware from spreading from computer to computer. As the years have passed, such threats have become less of a concern for many schools. "We feel that operating systems security—especially since Microsoft XP version 2—and products such as virus protection systems have improved, so it is now difficult for outsiders to break into our campus network," noted Tom Briggs, network manager at Northampton Community College in Pennsylvania, which has more than 30,000 students and staff.

The progress is welcome news, but security represents an ever evolving challenge, so it is not surprising that new problems are emerging. The nascent holes center more on internal security shortcomings than on threats from outsiders. This change is occurring because Web, e-mail, instant messaging, and peer-to-peer applications present easy outlets for accidental or deliberate leaks of confidential information. Increasingly, sensitive data can be compromised by just a few keystrokes, and often the transgressions leave no hard evidence (such as a paper trail or an electronic signature) behind, so academic institutions may not even be aware that a breach has taken place.

Many higher education enterprises are just beginning to recognize the extent of the problem. "Academic institutions have to rethink the way they view data security," said Ed Murrer, vice president of marketing at security software supplier Tablus Inc. "Employees may inadvertently leak information, and that could have significant ramifications for their institutions. They now have to take steps to safeguard internal correspondences." The problem is gaining traction so quickly that Gartner, a provider of research and analysis about the global information technology industry, predicts that in 2008, insiders, rather than outsiders, will account for the majority of the financial losses that enterprises will endure from unauthorized computer use.

What's Behind the Problem?

A variety of factors are coming together to create the problem. Academic institutions now hold a growing volume of sensitive information, such as credit card account numbers, employee Social Security numbers, and student grades. Increasingly, they have been automating the traditional methods of manipulating that information. While that change has meant they can process information more efficiently, it has also meant that the data can fall into the wrong hands more easily. "Employees may include confidential data in an e-mail message or an instant message without thinking twice about it," stated Raj Dhingra, vice president of marketing and business development at security software supplier PortAuthority Inc.

In fact, there were a number of instances in 2005 where sensitive data was compromised at colleges and universities. The University of Northern Colorado notified 30,000 students and staff members that their information had been compromised when a computer hard drive disappeared. The University of Chicago Hospital announced that an employee had been selling patient records to third parties. At Polk Community College in Winter Park, Florida, a professor was arrested for using students' names and Social Security numbers to obtain department store credit cards. Austin Peay State University, in Clarksville, Tennessee, exposed students' names, Social Security numbers, and other personal information to outsiders due to a problem with the search function on the school's website.

What's Being Done?

As awareness of such breaches increases, legislators are pushing organizations to more closely monitor internal communications. "The government has become proactive in passing a number of laws that require that schools safeguard sensitive information," noted Trent Henry, an industry analyst with market research firm the Burton Group. The Family Educational Rights and Privacy Act (FERPA) is a federal law designed to protect the privacy of students' educational records. The law applies to all schools that receive funds under programs sponsored by the U.S. Department of Education. In these cases, schools must obtain written permission from a student in order to release any information about that student's education record. Without that permission, the sharing of any confidential information is considered a criminal offense, and the university can be liable for damages.

The Health Insurance Portability and Accountability Act of 1996 requires that all electronic patient healthcare information be protected. "In many cases, schools have some medical information of their students on file and need to make sure it is safeguarded," stated Tablus's Murrer.

The federal Gramm-Leach-Bliley Act mandates that institutions dealing with credit cards provide sufficient privacy and protection of customer records. A growing number of academic employees access customer account and credit information, so by law, the institutions have to make sure that information is protected.

States are also ramping up with statutes dealing with the handling of personal information: California passed SB 1386, a law that mandates that all businesses protect personal financial information, such as credit card numbers.

In addition to these common types of sensitive data, schools generate unique forms of classified information. "Research data is important to academic institutions, and they would not want it to leak out," said PortAuthority's Dhingra. It therefore becomes imperative that schools protect their intellectual property by making sure that important data does not move from the university network to the Internet.

Identifying such problem transmissions can be difficult. While universities have set procedures with correspondences, such as invoices in an enterprise resource planning system, the fluid

▶

nature of e-mail and instant messaging means no one is sure when sensitive information may move from place to place.

"We are seeing a dramatic rise in the use of instant-messaging services among our users," noted Briggs at Northampton Community College. What is transmitted is not always clear in such cases. Because any employee—from an entry-level administrator to a university president—might unintentionally violate standard policies, every outbound message becomes suspect and therefore needs to be inspected.

New Tools Fix Some Problems

Traditional security products, such as virus protection systems, were not designed to guard against the emerging risk. New tools need to be able to monitor large volumes of outbound traffic generated from a variety of sources in real time without causing performance problems.

A handful of startup companies (Reconnex Inc., Tablus, Verdasys Inc., Vericept Corp., and Vontu Inc.) have stepped up to fill this new need, developing tools that enable organizations to monitor information as it moves beyond enterprise networks. Their products, dubbed secure content management (SCM) solutions, protect sensitive data by detecting, and sometimes blocking, messages containing confidential information that should not leave a school's boundaries. These tools apply security checks to information as it is about to leave the network. They open up the data and determine if it contains certain keywords or common patterns (such as ten-digit Social Security numbers) associated with sensitive data. If so, the products quarantine the information. Once information is quarantined, IT personnel or department managers can examine it to determine whether it should stay in the organization or can be released.

The products have different designs. Often they have an unobtrusive nature: The products sit on a network, watch information as it flows out of an academic institution, and flag questionable materials. Typically, vendors offer SCM appliances, hardware, and software attached to router ports that support wide area network connections. In other cases, vendors offer software solutions that sit at these points and watch the outgoing information flow. The tools need to be able to recognize sensitive data even if it has been modified, compressed, or encrypted. Consequently, the products need to recognize a wide range of data formats, including structured and unstructured data.

In addition to marking problem traffic, the tools need to help academic institutions figure out who is generating the data and how to stop inappropriate information flows. Consequently, SCM systems provide audit trails outlining when data moves out of an organization, who sent it, and whether or not it includes any sensitive data. Academic institutions can generate a variety of reports that examine information and search by date, sending client, or protocol. Ideally, the reports provide a tangible, quantifiable assessment of the risks an organization faces, including a summary of key findings and impact assessment, full details of each incident detected, and recommendations for minimizing the risk of data leakage.

Once an SCM system is in place, an institution should have a clear picture of its potential risk. "Organizations tend to be surprised about the volume of confidential information that is making its way out from their networks," said Peter Christy, an analyst with NetsEdge Research.

Typically, the problems stem from ignorance rather than malice. In a growing number of cases, employees need to send confidential information to themselves when they work at home or while they are on the road. In some cases, employees ship sensitive data, such as customer account information, electronically over unencrypted links, so it is open to outsiders. Usually after such questionable transactions are flagged, organizations take steps to protect the data. Employees need to make sure that they rely only on secure connections when sending themselves information.

"A lot of user training is required to make it clear how some of their habits may impact the organization," said the Burton Group's Henry.

While the products offer needed visibility into the growing problem of outbound leakage, they possess a number of limitations. Academic institutions face the question of how well such tools would fit with their primary mission.

"In the academic community, there is a great deal of emphasis on privacy and freedom of expression," noted Charles Morrow-Jones, director of system security at Ohio State University. "I could envision some resistance to products that would examine individuals' e-mail messages."

Installation, Policies, and Other Problems

Another problem is that products can be difficult to install. Academic institutions usually have multifaceted WAN networks with multiple entry and exit points. When an institution has multiple network exit points, it must set up SCM systems at each exit, collect the outbound transmission data, and then make sense of what is being transmitted. If an academic institution has segmented its servers so the confidential information is stored on a few systems, then SCM deployment becomes simpler.

Because each institution is unique, the type of information that it wants to safeguard is different. Consequently, customers have to develop policies that enable SCM systems to deduce whether information should stay inside or go beyond the network boundary. This means the products have to be customized for each installation. The tools can be set to monitor a variety of information sources: e-mail, instant messaging, peer-to-peer connections, and even spam. One firm discovered that confidential data was being transmitted via a Trojan horse that had made its way past the corporate firewall and was replicating itself within the company's network.

"While it can be easy to get the system up and running, it can be more difficult to make sure it is identifying only sensitive information," said the Burton Group's Henry. False positives, flagging information as confidential when it has been cleared, is an issue with these systems. While the vendors claim that false positive rates range from one to two percent, analysts put the number closer to the five to ten percent mark. As a result, false positives have the potential to slow an organization's information flow.

Another concern is how much information should be monitored. "Being able to sort through large volumes of data is essential to protecting intellectual property," said NetsEdge Research's Christy. "The broader the body of data that can be searched, the more the organization can be protected. The downside is the more information examined, the more likely the hit on throughput and network performance." With data exchanges becoming more complex—users at Northampton Community College want to attach 50MB files to their messages—performance problems could become more common.

Pricing for these products can also be prohibitive. While list prices start as low as $25,000, a typical installation price quickly reaches the $100,000 mark and a large, complex solution can cost $500,000. Since academic institutions tend to have large numbers of users, they will have to spend a lot of money to protect their networks.

Conclusion

Use of these tools is just beginning. Most customers have had them running in test mode and are just beginning to use them for large volumes of traffic, so questions about how effectively they handle these loads still have to be answered. While there are now many potential hurdles, vendors are expected to clear them, so use of the tools will spread. "In many cases, enterprises have no visibility into what information is being sent out of the firm, so these tools provide a necessary service, one that will grow in importance during the coming years," concluded the Burton Group's Henry.

Paul Korzeniowski is a freelance writer in Sudbury, Massachusetts, who specializes in networking issues. Reach him at paulkorzen@aol.com.

▼

Cell Phones, Land Lines, and E911

Are students more connected than ever, and yet more difficult to reach?

by Pat Scott

For most colleges and universities, providing phone service to students has become more complicated in the last year or two. Not so long ago this was a straightforward issue, and "one port per pillow" was highly respectable. State-of-the-art meant that each student had his or her own phone line and voice mailbox. Times were especially good because campuses could resell long-distance services, and telecom was highly regarded as a source of revenue, not just an expense.

Cell phones have changed everything.

A survey conducted on the Olivet Nazarene University campus is probably typical. In 2005, 81 percent of the students provided their own cell phone, according to Keith O'Dell, telecom manager. When one of the large Ivy League schools surveyed students, that percentage rose to 94 percent.

Staying in touch with friends is a way of life for most students today. They have grown accustomed to anytime accessibility, and they make regular use of instant messaging. The land line—in spite of the fact that it is reliable, comes with a clear signal, and is often included in the residence hall fees—is old technology that can't ride in a holster attached to anyone's belt when he leaves his room.

A New Set of Problems

One of the problems the migration to cell phones creates for schools is crisis management. Ideally, when a student dials 911 in an emergency using the land line, campus security or local authorities can locate the caller immediately. Not true from the cell phone. Most colleges are struggling with this because they have a responsibility for the safety of their students.

Another problem for school officials is getting in touch with students. When students bring their cell phones from home, calling them is often long distance from a campus phone, even if they're standing 100 feet away. If that's the only way to reach them, the campus phone bill becomes a budget buster very quickly, whether the calls are routine or related to some emergency situation.

Students who don't use the land line also do not always set up their voice mailboxes. So messages, urgent or not, that are sent to all students may or may not reach some students for days—if ever. Sandi Russell at Austin College in Sherman, Texas, says, "In January 2006, I checked every student voice mailbox and found that only 12 percent had set them up and only 5 percent were using them regularly. We will not be offering voice mailboxes or long distance to our students after June 1. We will recommend very strongly that, for safety reasons, parents not only bring a phone (answering machines will be allowed), but make sure it is plugged in. When students call 911 or our campus police, their location is shown in the display. If they use their cell phones, someone will have to be able to communicate to tell them where they are located."

Some campuses have considered exclusive cell-phone coverage. "We looked at this," reports Theresa Rowe, assistant vice president of university technology services at Oakland University in Rochester, Michigan. "What we did was end land-line service for all phones in residential areas. Phones in res halls are house phones—no off-campus or long-distance calls."

Alex Konialian, telecom analyst and wireless administrator at Towson University in Towson, Maryland, cautions, "Before removing land-line dialtone from the dorms, I would strongly advise consulting an attorney who specializes in risk management issues....I would never even think of terminating land-line dialtone in a dorm."

What's a Campus to Do?

KC Stevens, director of telecommunications at SUNY New Paltz, says they still provide land lines in the residence halls. "We built the cost of the residence hall phones into the room rent and now provide free local and long-distance calls. We bill the students for international calls and directory assistance only.

"We've found that this pleases everyone: administration, because we can still provide 911 in the residence halls and can still broadcast voicemail messages to every on-campus student; students and parents, because they don't have to deal with monthly bills; and telecommunications, because we bought ourselves time to decide our future direction," says Stevens. "We don't worry about cell phones or calling cards; we even bring in more revenue by leasing space on our taller buildings to the cell phone carriers. It's working for us."

That sort of plan works for Michigan Technological University as well, according to Jim Cross, who is now associate dean of the School of Technology at MTU. "Just the other day, I asked the 60 students in my class how many had cell phones," Cross says. "I think 100 percent raised their hands. Then I asked how many had more than one cell phone, and probably 10 percent of them raised their hands again. Some parents restrict usage on the one they provide, so these kids go get another one." Cross says MTU requires a phone in each dorm room for security. Dialtone and cable TV are included in the room fee, and students can choose to activate long distance for an additional fee.

Walt Magnussen, director of telecommunications at Texas A&M University, says he, too, still provides dial tone to each residence hall room. "Five years ago, we removed the phone instruments because they were just not being used. Students preferred bringing their own. We haven't done any formal study, but a very high percentage of our students bring their own cell phones when they come as well.

"We are still trying to find a solution to the mass communication issue. To send an e-mail to each student at A&M is a four- or five-hour process. So much for a timely response on this campus of 75,000."

Has A&M ever had an emergency that didn't get an adequate response due to cell phone usage? Yes, says Magnussen. "The last time we had a major crisis on campus was the bonfire incident in November 1999. Communications came to a standstill as parents and friends called in and phone lines became oversaturated, and cell phones became unusable due to the volume of simultaneous calls."

Magnussen cautions that laws vary from state to state, and colleges and universities have an obligation to know what the law says in their state. "Texas legislation changed about 10 years ago," Magnussen says, "and some schools still don't know what the law says. Residence halls have to have the same level of 911 (both ALI and ANI) that is required for the home. The law for business is not as stringent." Magnussen adds that the impossibility of adhering to different laws in different states is why there is a push for 911 for VoIP to be regulated at the federal level.

From the University of Scranton, Lisa Notarianni reports, "We are removing dormitory lines and using the funding to update the services that students use regularly, such as ResNet and cable TV. We are not implementing a distributed antenna system to guarantee 100 percent cellular coverage for all carriers. But, we are working with cellular carriers (only one at this time) to get towers on campus to enhance coverage and provide some supplemental income," Notarianni says. "We will look to add carriers as they find interest in building towers on our campus. For our student contact, we will use e-mail as our primary source of contact and will be implementing a requirement for students to enter their contact information (phone and address) before they can proceed with any other electronic services provided through the university. The data that we collect will be accessible only by staff and faculty and only used if e-mail is not effective for what they need. We are a Centrex customer, so the expenses associated with dorm lines are much greater than those with a PBX."

▶

"The ubiquitous connectivity device on campus is not the laptop—it's the cell phone. That's what students carry with them."

At the University of Toledo in Ohio, Carole Sedlock, telecommunications coordinator, says each room in the residence halls has dialtone, and 911 calls go directly to the Lucas County PSAP. The university is in the process of implementing "Conference 911" service, which will automatically conference in the campus police whenever a call goes out to 911 from campus. Calls from cell phones go to the county or to the City of Toledo PSAP, and it becomes the carrier's responsibility to send GPS location information. Bills now reflect a per-line fee to cover sending GPS information on 911 calls.

The Bearcat Phone at the University of Cincinnati

Facing down the challenges of the cell-phone dilemma, the University of Cincinnati has embarked on an ambitious next-generation solution to the problems of connecting to students, long-distance charges, and campus safety. If they meet their end-of-May deadline (and in late April they are on track), UC will provide each incoming freshman with a new Bearcat Phone at the freshman orientation in June. A cell phone on steroids, this device will accommodate unified messaging so students can retrieve e-mails, allow students to use five-digit dialing on campus, accompany them wherever they go, offer unlimited minutes at a bargain price, and provide location information if they need assistance from campus police.

Fred Siff, who is vice president and CIO at UC as well as a professor in the information systems department, saw students bringing phones from all different carriers and realized there was potential for improving service as well as gaining control over the somewhat chaotic world of cell phones. "When we realized we were still selling buggy whips, we knew it was time to change our business model," says Siff.

Reaching security in an emergency was a top priority issue. A handful of universities—five or six nationwide, according to Siff—have devised some sort of mobile help button. When UC held focus groups, Siff says that was the number-one application students wanted to see. "We are going to be offering cell-phone service, and we can guarantee 90 percent three-bar coverage on our campus. That becomes meaningful because you can't do that if you've got a whole bunch of different carriers with different levels of coverage. So going directly to our campus police becomes a very important application....On the high-end phone, it will be a button. On the low-end, give-away phone, students will probably have to press star and a number."

There are other applications that they felt were very important, Siff says. "We had to do something in the teaching space. On a university campus you cannot introduce technology just for technology's sake. It ought to directly impact teaching and learning. So what we're doing, in a word, is notification. We use the course management system Blackboard, and we are working with them to codevelop their mobility strategy application. Students would like to be notified when something in their course changes. The way it works now, a student will go to the Web and see if grades have been posted or announcements made. With the Bearcat Phone, they will get a text message telling them this has been done."

Siff says they also felt it was important that the student portal be the academic portal, the Blackboard portal. "So when they sign on, it says hello, here are the courses you're taking, and so on. We will port that onto the Bearcat Phone, and it will become the portal. That, too, is powerful because it has university information and is really the student's entry into the university. This is what will make the Bearcat Phone uniquely UC centered."

According to Siff, UC is also developing these applications to work on high-end Windows mobile devices. "We think faculty—and students as they mature and get more involved in their studies—will want to upgrade to a 'smart phone,' and we're going to provide an upgrade path. So all these applications will work on the cell phone, but they'll be even better and much richer on a smart phone."

Smart phones such as the one Siff describes can now cost upwards of $500, but he feels the prices will come down. Many UC faculty already use them. "The ubiquitous connectivity device on campus is not the laptop—it's the cell phone. That's what students carry with them. And the smarter and more productive we can make that device, the more it becomes the choice of professionals. Most professionals today have smart phones. Just as the PC back in the 1980s was a productivity device for professionals, today it's the smart phone. We like to see students thinking like professionals."

UC was hoping to have some time to do a pilot program with the Bearcat Phone—a dorm, a college faculty, a department. But the admissions department wanted to roll the program out with the 4,000 incoming freshmen: "Welcome to the university—here's your cell phone. You don't have to use it if you want to stay with the plan you came in with, but it has all these advantages."

Siff says they are working in partnership with Blackboard and Microsoft to develop all the applications, and they think they can meet the June deadline. "If we can put these things in the hands of the students, then what I think is the relatively minor problem of getting in touch with them becomes a by-product," he says.

Who will build the Bearcat Phone? In response to an RFP, Cincinnati Bell submitted a very strong proposal and is now building out the infrastructure. It is also providing the phones and the billing. In return, Siff estimates "thousands if not tens of thousands" of new clients.

Siff says he doesn't think they have all the answers yet, but he is certain they are asking all the right questions.

Conclusion

Obviously, new and converging technologies have thrown campus communications into a whirlpool. What will funnel out of the vortex and when remains to be seen, but it looks like whatever it is, it won't have a wire attached. While there are commonalities among the solutions to communications dilemmas, each campus is also unique and must find its own best answer.

Geoff Tritsch of Compass Consulting Division of Acentech offers these thoughts: "As technologists, we like to see issues in the context of technology, but what we're seeing here is not just a technology problem. We need to look at student communications in the broad context, in the long term, and in a whole new light. IT, telecom, residential life, campus security, deans, student services, health services, and others must all be part of the process. And what works for one school may not be the right solution for another. Location, culture, attitude, majors, and many other factors all play a part. Once you figure out what you are trying to accomplish, technology is the easy part. The hard parts include understanding what the students want, reshaping campus attitudes and procedures, and, of course, figuring out how to pay for it!"

Pat Scott is the ACUTA communications manager and editor of the *ACUTA Journal*. She never claims to be a high tech expert but always enjoys talking to ACUTA members about what's happening on campus. Reach her anytime (please!) at pscott@acuta.org.

▼

Interview

Jared L. Cohon, Ph.D.

Carnegie Mellon University

Jared L. Cohon became the 8th president of Carnegie Mellon University in July 1997. During his presidency, Carnegie Mellon has continued along its trajectory of innovation and growth, developing and implementing new and successful efforts in undergraduate education; information technology; biotechnology; the environment; the fine arts and humanities; diversity; and international education. In 2001, President Cohon shared Pittsburgh Magazine's "Pittsburgher of the Year" honors with Mark Nordenberg, chancellor of the University of Pittsburgh.

Dr. Cohon came to Carnegie Mellon from Yale University, where he was dean of the School of Forestry and Environmental Studies and professor of environmental systems analysis from 1992 to 1997. He started his teaching and research career in 1973 at Johns Hopkins, where he also served as Assistant and Associate Dean of Engineering and Vice Provost for Research. Dr. Cohon earned a B.S. degree in civil engineering from the University of Pennsylvania, and a Ph.D. in civil engineering from MIT.

In addition to his academic experience, he served in 1977 and 1978 as legislative assistant for energy and the environment to the Honorable Daniel Patrick Moynihan, retired United States Senator from New York.

President George W. Bush appointed Dr. Cohon in 2002 to his Homeland Security Advisory Council. He was also appointed as Chairman of the Council's Senior Advisory Committee on Academia and Policy Research.

Dr. Cohon is a member of the board of directors of Mellon Financial Corporation and American Standard, Inc. He also serves on the boards of several national and local non-profit organizations.

ACUTA: Since September 11, 2001, society has been less open worldwide. We have seen security increase at virtually all public events, at airports, and even on the Internet. How do you balance this increased need for security with the open environments that have historically been a source of pride on college and university campuses?

Cohon: The university is connected in ways unimaginable ten or twenty years ago, and with this new connectedness come new opportunities, new responsibilities, and new threats. The post-9/11 world is not only becoming flat, it is becoming smaller and more fluid; a world in which we need to constantly monitor the reasonable balance between academic openness and security, measures imposed on us and those we initiate. As a university, we have an obligation to promote inquiry and academic freedom. In order to ensure the flow of information, we must protect the flow of information. In order to encourage robust debate and healthy dialogue, we must protect the right of expression and privacy. In order to further research, we need to make certain that the quality of intellectual life is not impaired or distorted or that research and its dissemination is not diverted.

ACUTA: Most colleges and universities have limited financial and human resources to dedicate to a security strategy. Describe CMU's investment in its security program. How can even a small college deploy an effective security program on limited resources, and what might be the first priorities to address? What resources are currently available to shore up these security concerns?

Cohon: Carnegie Mellon created its information security office (ISO) in the fall of 2004. ISO reports to the chief information officer, with a dotted-line appointment to the university counsel. Six full-time security professionals provide incident response, training and awareness, tools and technology, policy development, and security assessment services. ISO also collaborates with faculty and researchers to advance the field of cybersecurity using Carnegie Mellon's computing infrastructure as a ready-made laboratory for study and testing.

Raising security awareness is perhaps the highest priority for an effective security program. It can be within the grasp of even the most constrained institutions by utilizing readily available resources such as the EDUCAUSE/Internet2 Computer and Network Security Task Force Cybersecurity Awareness Resource Library (http://www.educause.edu/CybersecurityAwarenessResourceLibrary/8762) and Carnegie Mellon Cylab's

MySecureCyberSpace (http://www.cylab.cmu.edu/default.aspx?id=1967). These and other freely available, high quality training and awareness materials provide an inexpensive solution to a critical element of an effective security program.

ACUTA: What should higher education's role in homeland security be? Regarding the FCC's ruling that the Communications Assistance for Law Enforcement Act (CALEA) potentially expands the wiretap law to all facilities-based broadband Internet access providers, do you also believe it is appropriate that colleges and universities be included under this law?

Cohon: Higher education has at least two roles to play in homeland security. One is to continue the basic research that will provide both security tools and insight into policies and procedures for using those tools wisely. The second is to continue its cooperation with agencies involved in homeland security when assistance is required. Higher education is already doing both; the only really new pieces are a change in research funding which has resulted in a shift toward more applied research and the question of CALEA compliance.

In terms of the latter, Carnegie Mellon shares the concerns voiced by many other colleges and universities and our professional organizations that the federal government consider ways to meet the goals of CALEA without forcing our institutions to incur hundreds of thousands to millions of dollars in IT expenses. Higher education has been a highly responsible and responsive sector in providing law enforcement agencies information they require; given both this fact and the limited number of requests that have come to our institutions over the last few years, it seems some middle ground on CALEA compliance should be possible.

ACUTA: Regarding Internet privacy, what do you think are the possible threats, what are our potential responses (either as a society or one institution), and how can we leverage technology to provide superior access to information and yet effectively address serious security concerns?

Cohon: The nature of the Internet presents a great challenge for those seeking to control access to their personal information. What sites individuals visit, with whom they interact, what they buy, and what they say can be readily captured, stored, shared, bought and sold, combined with other sources, and analyzed and manipulated to create detailed databases of personal information without the individual's knowledge, control, or consent. Targeted advertising, spam, identity theft, and stalking are examples of potential ill effects.

A full complement of both policy and technical strategies is necessary to effectively address online privacy concerns including legislation, user education, international agreements, and technology. Tools and technologies such as strong encryption, Web anonymizers, antispyware software, and firewalls and proxies reduce personal privacy risk without hampering access to information. Further, more widespread implementation of specifications such as the Platform for Privacy Preferences Project (P3P) coupled with user agents like Privacy Bird (http://www.privacybird.com/) will empower Internet users to make informed decisions to interact with Internet sites based on their expressed privacy policies. Ensuring Internet privacy must be a shared responsibility and collaborative effort between consumers and providers.

ACUTA: The well known and distinguished Computer Emergency Response Team (CERT) is a part of your campus. How did this center first come to your campus, and what impact has it had on your institution?

Cohon: The Cert® Program is a part of the Software Engineering Institute (SEI), a federally funded research and development center. In the fall of 1988 a college student created a "worm" program that infected ten percent of Internet systems and served as a wake-up call for network security. Following this incident, the Defense Advanced Research Projects Agency (DARPA) charged SEI to establish a center that would coordinate communication among experts to prevent future incidents. The charter of the CERT® Coordination Center (CERT®/CC) was to work with the Internet community to respond to security events, educate the community at large about security issues, and prevent security breaches.

As a result of the exponential increase in the size of the Internet, its use for critical functions, and the increasing sophistication of intruder techniques and potential for catastrophic damage, additional resources were needed, and CERT®/CC became part of a larger CERT® program. Other areas developed within the program include education and training, research and development, situational awareness, and global relationships.

▶

The critical thing to realize about the security challenge is that it has so many facets: technology, policy, organizational dynamics, privacy, education, and political choice. Any notion of a "magic bullet" or simple solution is an illusion.

ACUTA: CMU, like Texas A&M and others, has a branch campus in the middle east. Please share what this opportunity has meant to your campus and add any insight into other campuses that may be considering a similar undertaking.

Cohon: The campus in Qatar is well aligned with our core strengths in business and computer science, and also with our mission of service to society. The partnership with Qatar has enabled us to bring a stronger Middle East focus into our other education and research programs and has allowed us to broaden the experiences of our students in both locations. This past fall semester the class *American-Arab Encounters* was launched. Pittsburgh students and Doha students met twice weekly via videoconferencing to discuss the history of U.S.-Arab relations and current issues. They also participated in a weekly online discussion with a larger group of American and Arab students, facilitated by the nonprofit group Soliya, whose mission is to improve intercultural understanding.

We recently had the opportunity to introduce our excellent arts program to the educational community in Doha when the School of Drama streamed a live broadcast of its production of "Nathan the Wise" to members of the Doha campus, as well as students, faculty, and guests of the University of Qatar. G.E. Lessing's masterpiece, with its profound message of tolerance and understanding, afforded our students—both in Pittsburgh and Qatar—the opportunity to have a meaningful discussion of a critical topic of our time. Neither of these amazing, culture-bridging educational events would have taken place had we not had a presence in the Middle East. With the intense focus of the international community in the region, this may be the best time to be a part of the effort to effect a positive and lasting change.

ACUTA: Many of our brightest students come from countries that are plagued with terrorists. Since most if not all of these students share our concern with recent events, what do you do to prevent them from being typecast with others with whom they happen to share a nationality but not political beliefs?

Cohon: One of the advantages of working in a university setting is the opportunity to meet students, faculty, and visitors from all over the world. One of the responsibilities of a university, or any educational institution, is to take the inherent diversity of cultures, traditions, languages, and religious beliefs found on a campus and use them to foster an appreciation of differences, while recognizing that we share a common humanity. Diversity is a strategic priority we take very seriously at Carnegie Mellon, and we work very hard to create a sense of inclusion and community, particularly among our students.

ACUTA: Concluding our interview, our focus for this issue of the Journal is "Meeting the Security Challenge." Is there any special project at CMU that you feel would be of interest to our audience?

Cohon: The critical thing to realize about the security challenge is that it has so many facets: technology, policy, organizational dynamics, privacy, education, and political choice. Any notion of a "magic bullet" or simple solution is an illusion.

Carnegie Mellon learned many years ago that an interdisciplinary, multilevel approach to almost all problems is more effective. We are taking the same approach to both research in and implementation of security on campus. We have gathered under an umbrella organization called Cylab a collection of faculty and research scientists throughout the university who focus on everything from data encryption to privacy technologies to data mining to management and policy issues related to security. We believe the solutions will lie in the conversations and resulting collaborative work in which these scholars engage.

In the implementation of IT security on campus, we take a pluralist approach. We don't believe that firewalls or antivirus software or intrusion detection systems alone are the solution. Rather, we implement all of these things along with aggressive education of students in a mandatory class called Computer Skills Workshop about the new challenges and responsibilities in a less secure, completely connected world.

Carnegie Mellon offers education programs in security, including a professional master's degree in information security and an executive education program. We received funding from the National Science Foundation to organize the development of an information assurance capacity-building program (IACBP) in which we train faculty from other institutions (specifically historically Black colleges and universities and Hispanic-serving institutions). Funding was also provided by the Pittsburgh Digital Greenhouse (now called The Technology Collaborative) to create educational games for K-12 that promote safe and responsible computing (www.mysecurecyberspace.com).

We seek ways to use the results emerging from our research labs to inform our own institutional security efforts (e.g., having cybersecurity classes work with our information security office to audit our own systems and check for our own compliance with best practices). Information security is one of those places where Carnegie Mellon's long tradition of interdisciplinary problem-solving is the right approach for everyone addressing this challenge.

ACUTA expresses our sincere appreciation to Dr. Cohon for sharing his insights and experience with us in this interview. You are invited to visit the Carnegie Mellon campus at http://www.cmu.edu.

▼

Security Checklists

by Marjorie Windelberg, PhD

"To do" lists at work, "honey do" lists at home, grocery lists. Lists are useful tools for organizing and managing things. They help to ensure that we don't forget to take care of what's important. Security checklists serve a similar purpose, and they can also be used to benchmark your security practices.

Security checklists are one part of risk management, which is the set of activities by which an organization handles the probability and consequences of adverse incidents. Adverse incidents can affect the privacy or confidentiality of data, the integrity of data, or the availability of information and information systems. Risk management activities include assessing the risks and then deciding whether to accept the risks or to take actions to modify or mitigate the level of risk.

The actions to modify or mitigate risks are known as "controls" or "countermeasures." These controls are the basis for the security checklists presented here. There are different ways to categorize controls. One way is to divide them into management, operational, and technical controls. Controls can also be categorized as to whether they prevent incidents, detect them, or help in the response and recovery.

Management controls, operational controls, and technical controls are further defined in the following sections. Each section also has a list of controls and some sample questions for evaluating the effectiveness of the control.

Management Controls

Management controls are those for managing risks. Management controls cover policy and planning for security management as well as assessing risks and auditing or testing security measures. Managing systems and services also comes under the heading of management controls.

Policy and Planning

Policy

- Does the information security policy address purpose, scope, roles, responsibilities, and compliance?
- Are standards of reasonable care and due diligence required?
- Are penalties and consequences for failure to follow policies enumerated?

Planning

- Are security plans required for all systems, including networks?
- Are regular reviews and updates to plans required?

Budget

- Is there adequate funding for security, including personnel, operations, and new acquisitions?

Risk Assessment

Policy

- Is risk management required, including performance of risk assessment and planning for mitigation activities?

- Is periodic review and update of assessments and plans required?

Classifications of information and systems, including network infrastructure

- Is sensitivity of information (personal privacy or intellectual ownership) identified?
- Is information classified as to how critical it is to the organization's mission?
- Are information systems and network infrastructure components prioritized for protection as well as recovery?

Security Assessments and Audits

Policy

- How frequently should they be performed? What scope is needed?
- Does an independent third party evaluate the security architecture and controls?
- Are tracking of deficiencies and plans to correct them required?

Testing and Monitoring

- Are systems scanned periodically and after changes for vulnerabilities such as default configurations, misconfigurations, or unpatched systems?
- Are systems monitored to ensure that only allowed processes are running? Are firewall rules reviewed and periodically updated?
- Are password cracking tests run to identify weak or easily guessed passwords?

Systems and Services Management

Policy

- Is information security required to be considered for all IT systems and services, whether purchased or developed in-house?
- Is compliance with all laws and regulations required? For example, are laws with respect to copyright or child pornography referenced?

Documentation

- Must security procedures, guidelines, and standards be documented? Are they?
- Are they reviewed and updated as needed?
- Are they audited or tested as needed?

Purchasing

- Are security standards required as part of any purchase of information technology products and services?
- Are vendors evaluated for their security capabilities?

Architecture

- Does the approach to security include redundancy and layers of defenses?
- Is the architecture designed – as opposed to resulting from reactions to threats and vulnerabilities over time?
- Is the architecture periodically reviewed?

Interconnections

- Are formal agreements required for connections or data exchange with external parties? Are external parties evaluated for their security capabilities?

Operational Controls

Operational controls are typically procedures that people implement or execute in a variety of areas. One is systems operations and management and the associated discipline of configuration management. Incident response and business continuity are also forms of operational controls. Other areas are personnel management, including security awareness and training, and a myriad of forms of physical security.

Security Operations and Maintenance

Network and System Administration

- Are unused ports closed? Are systems hardened? That is, are programs and utilities associated with unneeded services deleted?
- Is the use of FTP limited?

Vulnerability Notification

- Do system and network administrators monitor both vendors and public sources for information on vulnerabilities and availability of patches?
- Are these advisories prioritized and acted upon in an appropriate time frame?

Fault and Problem Management

- Is there testing for system defects and errors? Are information system defects and errors tracked and corrected in an appropriate time frame?

Patches and Upgrades

- Are security patches and upgrades installed in a timely manner?
- Are they tested prior to installation?

System and Media Disposal

- Are media properly wiped or destroyed for disposal?
- Are paper records with sensitive information, including security settings, shredded rather than thrown out?

Configuration Management

Policy

- Is configuration management practiced?

▶

- Are inventories of hardware and software complete, accurate, and up to date?
- Are configurations reviewed and audited periodically?
- Are default settings and default passwords changed when systems and software are installed?

Telecommunications

- Is access to outside dialtone blocked for trunks connecting the voice system and the voicemail system? Are unused voicemail boxes removed promptly?
- Are trunk-to-trunk transfers disallowed?
- Is call forwarding to off-premises numbers disallowed?

VoIP

- Is the ability to log in remotely to VoIP phones, servers, and gateways limited?
- Are direct connections to the Internet blocked?

Change Control

- Are change management procedures required?
- Are changes to systems reviewed and authorized?
- Are only authorized personnel allowed to install or change equipment or software?
- Are emergency change procedures available but used only rarely?
- Are procedures for backing out considered as part of the installation process? Is a test lab used to test changes and restore procedures?

Incident Response

Policy

- Is there a policy that establishes incident response planning and other capabilities?
- Does the policy require incidents, including losses, to be reported?
- Is the plan reviewed and updated periodically?
- Are components of the plan tested regularly?
- Are staff members trained for incident response?

Handling

- Are standards for investigating incidents set?
- Do standards address involvement of law enforcement?
- Do they include procedural protections for suspects?
- Are post-incident reviews required?
- Are they actually conducted, to capture lessons learned?

Business Continuity

Policy

- Is a business continuity plan required? Is the plan updated regularly?
- Is testing of the business continuity plan required?
- Are appropriate people trained to follow the business continuity plan?

Alternatives

- Is there route diversity and redundancy in the network configuration?
- Is there an alternative site for processing?

Backups and Restores

- Are systems backed up regularly?
- Are backups stored off-site?
- Are restores from backups tested periodically?

Personnel

- Are background checks required for employees, temporary workers, and contract workers who handle sensitive data or administer critical systems?
- Is separation of duties required?
- In handling termination situations, is cooperation between human resources and information technology departments required?
- Are standards for termination set?

Security Awareness and Training

- Does a policy require security training and awareness programs?
- Are users fully trained in security awareness and risks associated with information technology?
- Are users required to take security training annually?
- Do technical staff receive appropriate quality security training?

Physical Security

Policy

- Is physical protection addressed in policies?

Access to Sensitive Areas

- Do doors have locks?
- Are doors checked regularly?
- Are cameras and/or sensors used for surveillance?

Network

- Is cabling sufficiently protected?

Alarms

- Are alarms in place?
- Are alarms monitored?
- Are there procedures for responding to alarms?
- Are alarms and monitoring procedures tested?

Environment

- Is there emergency power and lighting?
- Is there fire protection?
- Are there sensors for temperature and humidity?
- Are there protections against water damage?
- Are there emergency shutdown controls?
- Are environmental controls monitored and tested?

Technical Controls

Technical controls are primarily implemented and carried out through hardware or software mechanisms. In addition to the basic objective of protecting networks and systems, technical controls include identification, authentication, and access controls. Finally, mechanisms for ensuring auditability and accountability are also technical controls.

Protection

Encryption

- Is encryption required for sensitive information?
- Are data transmissions encrypted?
- Are records or files with sensitive data encrypted when stored?
- Are log files encrypted?
- Is VoIP call content encrypted?

Malicious Code and Hackers

- Is antivirus software deployed and kept updated?
- Is antispam antispyware software deployed and updated?
- Are firewalls used and kept updated?
- Is intrusion detection or intrusion prevention used?
- Are IDS signatures updated regularly?
- Is a file integrity checking tool used?

Identification and Authentication

Users

- Are shared or group accounts disallowed?
- Are users required to provide identification and authentication (e.g., account name and password or PIN) before accessing resources?
- Is the use of guest and anonymous accounts or access controlled?

Devices

- Are devices authenticated (e.g., with a MAC address) when attaching to the network?
- Are RADIUS servers used?
- Has 802.1x been implemented?

Passwords

- Are strong passwords required?

Access Controls

Authorization for Use

- Are access control measures required by policy to protect information and systems?
- Who may use data and information systems?
- For what purposes may they use them?
- What activities are prohibited? Who may operate or administer systems?

Mobile and Remote Use

- Is remote access addressed?
- Is wireless access addressed?
- Are portable devices such as laptops and PDAs addressed?

Account Management

- Are unused and idle accounts tracked and shut down?
- Are temporary accounts closely controlled?
- Is administrator, root, or super user access limited to only the few people who have those responsibilities?

Unsuccessful Logons

- Are unsuccessful logon attempts tracked?
- Is an account locked after the threshold for unsuccessful attempts has been exceeded?

Session Controls

- Is a session locked after being idle?
- Is a session terminated upon disconnect?

Logs and Audit Trails

- Are logs and audit trails enabled?
- Are logs and audit trails reviewed for anomalies promptly and regularly?
- Is traffic analysis done regularly?
- Is audit information protected?

Audit

Wireless

- Are scans for unauthorized wireless access points performed?
- Are wireless access points reviewed to find ones that are not properly configured?
- Are wireless packets examined to verify that they are using the standard authentication protocol?

Telecommunications

- Are trunk restrictions reviewed?
- Are voicemail boxes and access reviewed for hacking and patterns of misuse?
- Are IVR setups reviewed for patterns of misuse?
- Are call detail records and phone bills reviewed for evidence of abuse and fraud?

VoIP

- Do you review firewall log to determine types of calls and whether calls are changing type during the call?

Conclusion

You don't have to look very far to find someone who has experienced a disaster of some magnitude. (Do you live anywhere near the Gulf Coast?) If you haven't reviewed your own security checklists, perhaps *now* would be a good time for that review.

Marjorie Windelberg, Ph.D., teaches graduate-level courses in information assurance and homeland security for the University of Maryland University College. An active contributor to ACUTA publications and a frequent presenter at ACUTA events, she can be reached at mwindelberg@earthlink.net.

▼

Higher Ed's Tricky Equation: Directories Help Balance Availability with Security

by Luci Norlin

According to the 2005 Campus Computing Survey conducted by the Campus Computing Project, network and data security was identified by campus IT officials as a key issue that will affect institutions over the next few years. Half of the institutions participating in the survey had experienced hacks or attacks on their campus networks in the past academic year, 41 percent had suffered major spyware infestations, 35 percent had experienced major viruses, and 20 percent reported security incidents involving identity management.

"The data confirm that network and data security are major concerns for campus IT officials across all sectors of American higher education," said Kenneth C. Green, founding director of the Campus Computing Project. "The 2005 data also document a major shift in campus IT priorities from instructional integration to security and enterprise resource planning (ERP)/infrastructure issues."

The challenge arises from the difficult balancing act that college and university CIOs must master today: On one hand, campus resources must support academic freedom and interactive learning environments where students, professors, and researchers can access, share, and publish at will. On the other hand, this highly prized openness makes universities targets for cyber break-ins and other unauthorized uses of institutional resources, including rogue use of both physical spaces and digital data.

With both physical and data security a top priority for most higher education CIOs, a growing movement is taking place to create more holistic approaches to campus identity and access management (IAM). Washington, D.C.–based Howard University deployed just such an approach, integrating a package of security management solutions from Siemens Communications that includes physical control and monitoring technologies as well as sophisticated identity- and access-management systems.

"There is considerable value in deploying a converged security solution for logical and physical access," said Datamonitor security analyst Tim Gower. For example, by deploying an integrated smart card security solution for both data and physical access, Gower's firm estimates that an enterprise may save more than $2 million annually for every 2,000 people covered by such a combined IAM system.

According to a Datamonitor survey of 53 organizations, substantial cost savings result not only from the protection of resources and data, but also from such factors as reduced time spent on sign-on procedures, better management of PKI certificates, consolidation of access privileges onto multifunctional smart cards, easier card provisioning, and reduced numbers of password-related queries made to IT departments.

This same logic can be applied to universities and colleges, whereby IAM comprises the creation, maintenance, and administration of identities as well as the permissions and policies that determine who gets access to what and under what circumstances. The process of digital identity management combines authentication, in which end users are challenged to prove that they are who they say they are, with authorization, in which an individual or group identity is matched with a set of access rights to various systems and files.

Directories Play a Crucial Role

Clearly, directories play a crucial role in the security architectures of colleges and universities. However, the problem is that there are too many of them. Such directories contain redundant sets of user IDs and data. And they are managed separately, with different tools and commands. Adminstrators struggle to maintain consistency between entries and must keep track of user access rights across multiple systems and accounts. Such synchronization of data among directories is a time-consuming, often manual job.

IT administrators are severely hindered in their ability to identify and plug security holes as well as provision and deprovision user-access rights in a timely manner. As a result, academic institutions are increasingly using *meta-directories* as the basis for campuswide IAM infrastructure. From a manageability perspective, meta-directory platforms provide the umbrella infrastructure to synchronize and tie together disparate directories and allow IT managers to centrally administer IAM throughout all applications and security systems—all from a single console. Meta-directories are vital for storing, maintaining, and updating identities and related information. The information they house can be used for reference purposes, user authentication, and access control.

Meta-directories help strengthen an academic institution's defenses against growing security threats—inside as well as outside the campus. Here's how:

1. Rapid provisioning and deprovisioning. Access rights can be provisioned for incoming students, faculty, and visitors—as soon as they arrive on campus—and can be deprovisioned the moment they leave. The meta-directory's dynamic links to all relevant directories and security systems ensure that no resources will be overlooked. This minimizes the likelihood that a departing end user will

▶

What Is a Meta-Directory?

In computer language, a directory is a part of a file system that contains a group of files and/or other directories (called subdirectories). In the same way that an office might have an entire room dedicated to a vast filing system, a computer file system may contain thousands of files. Directories help organize them by keeping files that are related together.

A meta-directory is "nothing more than an architectural concept that covers the issues necessary to implement an umbrella directory over other directories....A directory becomes a meta-directory when it's used as the focal point to manage other directories," says Michael Chacon at MCPMag.com.

From a technical perspective, there are two main approaches to meta-directories, explains Chacon. One is *synchronization* of data stores, in which information is replicated from one data store to another. "This is a necessary feature of an independent directory service, such as NDS or AD, in order to maintain accurate and authoritative information within the distributed databases that make up the respective directories," says Chacon. "However, for the meta-directory, synchronization-specific information in each independent directory must be replicated to the other."

The other approach is *chaining*, or *brokering*, in which data is retrieved from another data store but the local data store is not updated. To fulfill a request for information, the system looks to the authoritative source.

("Meta-Directory Mindset," April 2000, http://www.mcpmag.com/columns/print.asp?EditorialsID=167) retain, and possibly abuse, access rights to campus systems data.

2. Centralized management. Administrators can monitor and control user access across all IT systems from a single console. This allows for quick and proactive response to potential security breaches.

3. Granular, policy-based control. Meta-directory IAM platforms use preset policies to determine who gets access to what on an increasingly granular level. This is crucial to institutions of higher learning. Adminstrators need to provision access privileges according to the various student, professor, and visitor roles.

4. Control of both logical and physical resources. More and more campus environments are working toward a single sign-on or single password approach for both logical IT resources and physical facilities. This is done by connecting meta-directories to smart card systems to control access to dormitories, computer rooms, laboratories, libraries, and other restricted campus areas.

Selecting the Best Meta-Directory

Meta-directories are critical components of effective IAM solutions, providing both openness and security to numerous types of users. When choosing a meta-directory solution, characteristics to look for include the following:

- High performance. As a central clearing house for identity information across the enterprise, the meta-directory needs to be able to respond to multiple simultaneous queries, authentication requests, and user information updates in a timely fashion, even during peak traffic hours.
- A scalable, flexible architecture that can be tailored, configured, and reconfigured to meet specific needs. In addition to campus user populations, many colleges provide information resources, in a secured fashion, to commuting and even telecommuting students, as well as to alumni, other schools, and the public. Furthermore, an organization might have millions of ID entries or a few hundred, a couple of workgroup directories or one huge global active directory (AD), or a hundred different directory-enabled applications.
- High availability and reliability. Given the critical role it plays in an organization's IAM infrastructure, a meta-directory platform should be equipped with business continuance features such as automatic backup and restore, redundancy, and a centralized console for performance monitoring and troubleshooting.
- Standards support that enables the meta-directory to communicate with other standards-based systems without the need to write special links or scripts. For example, most directory-enabled applications use Lightweight Directory Access Protocol (LDAP), a standard that enables clients to interact with a directory (or directories and a meta-directory to interact) for authentication and profile retrieval.
- Proprietary support. Not all systems and applications support LDAP; therefore, the meta-directory needs to support a full range of vendor-specific application programming interfaces

(APIs). For example, Windows server management applications often use Microsoft's NT Sequential Access Method or Active Directory Services Interface APIs. Even if a directory supports LDAP, proprietary APIs tend to support richer functionality than generic LDAP-enabled applications.

- Integrated modules. A meta-directory platform works best as a suite of integrated functional modules, starting with a basic platform and adding modules as needed. A typical initial deployment would consist of the meta-directory engine, a data store, and a hub that ties everything together. Later additions might include automated workflow and additional agents that link to proprietary, directory-enabled applications.
- Interoperability. A meta-directory should be able to run on top of all the popular operating systems, including Microsoft Windows, Linux, and various Unix platforms. This allows IT staffs to deploy the meta-directory on the operating system they and end users are most familiar with, for which a support structure already exists in the organization.

Conclusion

When students go away to college, they prepare to master tough equations while striking the right balance between academic and social life. Hardly anyone in this group realizes that the chief information officers at these places of higher education are also working to create a perfect balance—not between prioritizing assignments and seeing all their friends, but between providing appropriate access to information to faculty, staff, and students on the one hand and denying access to those who would cause mischief or commit crimes on the other.

Luci Norlin is the national higher education business development manager at Siemens Communications Inc. Reach her at luci.norlin@siemens.com.

▼

acuta

35th Annual Conference and Exhibition

July 23–27, 2006

San Diego, California

Manchester Grand Hyatt

> The information gained from the sessions and especially the interaction with others is fabulous. I go away from the Conference each year with more confidence in my knowledge and abilities.
>
> *Gail Stephens*
> *Radford University*

www.acuta.org

57 Reasons You Should Attend ACUTA's Annual Conference

Preconference Seminars

Business Continuity & Disaster Recovery Planning for Higher-Ed Institutions
(David Kim, Tina Koopmans, Ron Walczak)

The Changing Landscape of IT Threats & Security
(Todd Halperin, Gerry Soderstrom)

The Convergence of Communications & Construction
(Tom Rauscher)

Keynote/General Session Speakers

Technology Imagination, Your Future & the Edge of Something New (Thornton May)

Lessons Learned from Hurricane Katrina
(Nancy Victory, Brian Voss)

Legislative and Regulatory Update from Washington
(Mark Luker, Jeff Linder)

Change: The "Real" Fear Factor–When Change Happens to Good People (Judy Carter)

Breakout Sessions

Case Studies of IPT Deployment
(DeAnna Moore, Jeff Early, Tim Winders)

Communicating Effectively through the Use of DiSC
(Gary Talbert)

Communications Infrastructure Budgeting & Planning at FSU
(Charles Friedrich)

Implementing a Mobile Phone Program
(Raju Rishi, Edward Chapel)

Lessons Learned in the Implementation of VOIP
(Bill Winn)

New Federal E911 Laws for VoIP
(Larry Foster)

Next Generation Technology–What it Takes
(Angel Dronsfield, Tamara Closs, Jim Dancer)

The Future Residential Campus: The 21st Century Project
(Michael Coakley, Sallie Traxler)

VoIP Basics
(Walt Magnussen)

Web Portal Technology
(Jameson Watkins)

Whole Building Design Solutions
(Geoff Tritsch, Ernie Schirmer)

At the Edges of Disaster
(Tina Koopmans, Corinne Hoch, Brian Voss, Travis Berkley)

Building an IT Security Architecture & Framework
(Mike Gibbs)

Expanding Wireless Technology on Campus
(Ron Walczak)

Implementing a Disaster Plan at NIU
(Teri Reid)

Meeting Communications Needs through VoIP
(Jim Spriggle)

Open Source IP Telephony
(Jose Valdes)

Planning to Meet Future Communications Needs
(Mark Reynolds, Sue Platner, Michele Norin)

Realignment of Telecom Contracts
(Garret Yoshimi)

Selecting & Implementing a Telemanagement System
(Michele Norin, Ann-Marie Lancaster, Susan Faulkner)

Unified Messaging Tips and Traps
(Mahendra Soneji, Ben Crown)

VoIP – Can We Talk? (Facilitated Discussion)

A Funding Model for a Converged Network
(Naila Machado, Mike Palladino)

A Strategic Approach to Information Security
(Dave Kovarik)

ACUTA Legislative & Regulatory Priorities
(Dave Ostrom, Jeff Linder)

CALEA Issues
(Mark Luker, Greg Seibert)

Central Cost Recovery at KUMC
(Matt Fuoco, DeAnna Villarreal)

Communication User Charges at UCSD
(Eddie Mardon)

Converging Entertainment & Technology to Create Community
(Cindy Phillips, Farrell Reynolds)

Enabling an All-IP Real-Time Communications Infrastructure
(Christian Schlatter)

How & Why ENMU-Roswell Went Digital Voice
(Art Leible)

How to Communicate with Executives
(Sue Workman)

Hybrid PBX - VoIP Solution at Georgetown
(Donna White)

NLR & Other Research Projects
(John Moore)

Solutions for Individuals with Communication Disabilities
(Bill Stobbe, Judy Viera)

Structured Cabling Standards - Evolving with Migration
(Jason Krauskopf)

VoIP Research
(Walt Magnussen)

Documentation & Installation of Communications Infrastructure
(Bruce Cotsonas, Todd Strand)

Meeting the Demand for Wireless Connectivity
(Nate Walker, Mike Ruiz)

Navigating the Technology Procurement Process
(Douglas Carolus, Scott Claverie)

Corporate Presentations

Beyond Unified Messaging, What's Next?
(Neal Shact, Fred McConnell)

Trends in Wireless Security and Intrusion Prevention
(Rohit Mehra)

Three Essentials in Emergency Event Management
(Kathy Veldboom)

Connecting the Campus – A Convergence Process
(Frank Vaskelis, Michael Lewis)

How to Move your Call Centers to IP
(Terry Dunigan)

Ideas that Communicate
(Steve Witt)

Deploying 10GBASE-T Cabling
(Hugo Draye)

Reach Anyone with Speech-Enabled Auto Attendants
(Terry Griffin)

The Convergence of IT & AV
(Richard Tregaskes, Graham Naylor-Smith)

Using Traffic Management Solutions
(Larry Schmidt)

> “Of all the associations that exist today, only ACUTA focuses on the specific challenges faced by those of us who provide voice, data, and video services on campus. ACUTA programs focus on what we need to know in order to serve our institutions effectively. Attendance at ACUTA events is a crucial part of my own professional development as well as others on my staff.
>
> *Matt Arthur*
> *Washington University at St. Louis*
> *ACUTA Program Chair*

Disaster Recovery Planning Essentials

Catherine McNair

Can't get any budget money to plan for a disaster? If your organization is like many others, any disaster recovery budget money available is already tied up in protecting the data infrastructure. You and I both know, however, that protecting the voice capabilities of your organization is just as important—and sometimes even more so.

Until you can get approval for more money, what can you do? Plenty. Although you recognize the need for equipment upgrades and adding redundancy, and haven't a spare minute to spend on all this, there are a few things you can and should do.

Cover the Basics

Wherever you are in the planning stages, don't forget a few important basics. The first is to run through a test of whatever level plans you have. No disaster recovery planning effort is complete without testing how well it will work. A mock drill, a tabletop exercise, or an actual out-of-hours simulation uncovers gaps in the planning that you can fill before a disaster happens. Some disaster recovery consulting service companies will do a short drill for a very reasonable fee.

The second is to put a copy of your documented plan off-site. Whatever you have documented, it is essential to have a copy off-site. Keep a copy at an alternate site—your home, a document-storage facility, or your car. Just don't have the only copy in your office, in case you aren't able to get into your office. Disaster recovery professionals insist that if the document doesn't exist off-site, it might as well not exist at all.

Use What You Have

There will probably come a time when you will be requesting budget money for additional disaster recovery planning or infrastructure upgrades to make your equipment more reliable and survivable. It will be to your benefit to show how you've already exhausted efforts to use what you have in place today. Take the time to begin a few simple activities such as ensuring that you have system backups and reviewing the capabilities of your telephone system for disaster recovery uses.

The following bears mentioning because it costs so little: Have extra backups of your voice system configuration and rotate that media off-site. Rotate those backups on a regular basis. Store them off-site even if you have to take them home. If the on-site backup is destroyed, you could save the day if you had the foresight to make another one and take it off-site for preservation.

Take a look at your voice systems with an eye toward enhancing your ability to automatically recover from failures and to improve your system's ability to support emergency response efforts. You may find features or capabilities that can be enabled, methods of improving call-routing strategies, or other changes that can be put in place with little to no cost. Some questions to consider might include:

From the website of the University of Georgia in Athens: http://www.infosec.uga.edu/

The Five A's of Security

Underlying a successful security program is a comprehensive security policy that defines the details for command, control, and compliance and provides a road map for maintenance as the program matures.

The five A's act as general guidelines:

Administration: Determine who will maintain, modify, and monitor security policy information.

Authorization: Insist on providing only authorized access.

Asset: Keep all information confidential.

Accountability: Make sure you can track and monitor who performs transactions at all times. Be able to determine if these transactions are appropriate.

Assurance: Understand that the survivability of your program is related to the survivability of your security policy and vice versa.

- Can you create a fast way to redirect calls internally if you have to leave a building suddenly? A button on an operator console that call forwards a main or a DID number to an alternate number, auto attendant, or voicemail allows personnel to redirect calls and exit the building quickly. Remember—these abilities depend on the system being available. If the system is shut down, you must use other means to redirect calls. You may have different procedures for redirecting calls depending on whether the system is available or not.

- Do you have extra equipment that can be set up for emergency use and stored at an off-site location? This may be phones, circuit cards, or even a spare system no longer used.

- IP (Internet protocol) telephony technology can add diversity to the communication methods your system uses. The ability to utilize the data network as a communication path provides an alternate path to complete phone calls or other applications. If you have already implemented IP telephony, consider how this capability might be used to provide an alternate communication path for users.

- Do you have a way of identifying the location of a 911 caller? For example, features such as Avaya Communication Manager's crisis-alert can help—when properly administered, it sends an emergency alert to a designated phone whenever 911 is called. This feature can be enabled very quickly at no additional cost. For more advanced needs, E911 products and services are important to consider for human safety. If you're not fully prepared to identify a caller's location to emergency response teams, this alone may be enough to warrant a budget approval to protect students, administrators, and educators.

Michael Crisler, program manager for public safety and cybersecurity for Miami-Dade County in Florida, has put detailed procedures in place to protect the media servers at the Office of Emergency Management EOC (Emergency Operations Center) when disaster strikes. During recent hurricane seasons, when the Florida coastline was threatened by multiple hurricanes, these procedures were an important safeguard to the county's continued business operations. "One of many levels of protection the county has in place is a comprehensive review of our EOC telephones when the hurricane warnings come in," said Crisler. "The review includes checking all call-forwarding in place, creating new backups so recent changes are not lost, and many other aspects of the system configuration. This allows us to proactively get the system back to the state it was in before the hurricane and lessens the impact on our users." A simple checklist review such as this one can be used when there is time to prepare systems for downtime. And, users experience seamless operations.

Although your situation may not exactly fit these examples, my hope is to spark ideas for ways you can use the system you have to your best advantage.

Get Out and Meet People

Telecommunications managers tend to be lonely. We end up with basement offices away from our coworkers and often avoid them because that's just an

▶

opportunity for complaints. Don't avoid certain kinds of contact with your peers...they can help you.

Get to know business continuity people. Assuming that this isn't you, one person in your organization you definitely want to get to know is the business continuity planner. This may be a person with the title of business continuity manager or something similar, or it may be an IT manager or an executive with responsibility for continuity of business operations. This person can do two things for you: He or she influences how disaster recovery money is spent and possesses knowledge you need.

Other business continuity professionals can be found at local groups such as a chapter of the Association of Continuity Planners, or organizations such as Disaster Recovery Institute International and International Disaster Recovery Association. Each of these organizations has a website with resources and contacts. In addition, the *Disaster Recovery Journal* is an excellent source of articles, information, and online references.

Get to know other communications technology professionals. You're already doing this by your involvement with ACUTA and by reading this journal. ACUTA seminars and conferences often offer sessions specific to business continuity and disaster recovery. At these sessions, you learn strategies as well as what other communications managers are doing. Organizations like this can provide valuable contact with other communications professionals.

There are also user groups specific to vendors you work with. Even if you just begin contacting other communications managers informally to discuss ideas or concerns, you are collaborating and sharing ideas that could benefit your organization.

Start Writing

Don't skip this section because you hate to write (or you don't have time). One of the most important disaster recovery planning exercises you can do is to document information that will be needed for recovery efforts. Even if you are starting with no disaster recovery plan at all, you can prepare information that may be very valuable if a disaster occurs. Begin by documenting equipment or assistance that will be needed in a recovery effort, and store a copy of these documents off-site. When you do seek funding for business continuity and disaster-recovery work you know is necessary, having documented as much as possible will put you ahead. You'll have a clearer idea of the most vulnerable areas of the infrastructure so you can prioritize what is needed. You will also have a clearer idea of where you need assistance from outside the organization, such as from a consultant to help your planning efforts, or hot site vendor to provide an alternate recovery site.

Begin documenting by creating an inventory of all equipment you currently have, along with the vendor that maintains it. Include serial numbers, contact information for the vendors, and other pertinent information such as contractual issues, costs, or account numbers. Document your power and wiring infrastructures. And—very important—document anything you know about the impact of a disaster. If an area of your business is vulnerable, document where and why. For instance, if you know that during registrations, the financial aid department cannot be without phones for more than a certain amount of time, and that if there were an outage the public impact would be unacceptable, then detail this information for those who hold the purse strings. Showing a significant financial impact will improve your chances of gaining approval for the improvements you need to make.

You might feel you do not have time for these tasks. You may need to simply focus your efforts on documenting what you know about the impact of an outage; document the efforts you have made and include everything you know about what the costs would be if a disaster occurred. The impact of a disaster will cost more than infrastructure improvements or a consultant to help you. Armed with specific information, you have leverage to obtain funding for the disaster recovery efforts you know are necessary. In the meantime, you can satisfy your conscience by doing your best to protect the infrastructure so critical to the success of your organization.

Catherine McNair is a certified Associate Business Continuity Planner (ABCP) and a business continuity consultant with Avaya Inc., with over 12 years of experience in designing and implementing telecommunications solutions for enterprise businesses. Reach her at catherine.mcnair@earthlink.net.

▼

Passing the Test of Productivity

by Mick McKellar

My first PC was a Commodore PC10-2 with two 5.25" floppy drives, and it ran at "turbo speed" of 10 Mhz. With a 1200-baud modem, I could have sent text messages—had I known anyone who could receive them.

We've come a long way over the years. Everything is much smaller, much faster, more powerful, more interconnected, more integrated, and more mobile. Convergence is upon us, and a cell phone may now also be a PDA, text messenger, camera, music and video player, Web browser, and e-mail station. I applaud the ingenuity of the designers; however, in the name of progress we must be careful not to impede productivity—not every change improves the bottom line.

Sacrificing Usability

Here's a difficult thought for the technophile: In the very competitive world of high technology, it's easy to fall into the trap of trading usability for gadgetry. Applications overlap features and duplicate capabilities. Installing one application adds buttons and plugs to other applications. On most of our systems, there are at least seven different ways to generate a PDF file from text, depending upon the application used to open the file. A PC talks to a PDA, PDAs talk to each other, and cell phones talk to everyone.

However, if a colleague sends an old-fashioned e-mail, it could arrive on all four devices at once. Removing an unwanted message from one device does not necessarily remove it from all of them. It might also be on the network or on the server of your ISP and remain there until it suddenly appears once again, unexpected and ill timed.

The complex interaction of PC applications and the varieties of hardware may make the gadgets we purchase less useful than if we could easily categorize their functions. Do we really need a phone that doubles as a camera and a voice recorder? Should we be running the batteries down while listening to music at our desk? Those who love technology for technology's sake should have input into purchasing decisions but may have to be reminded that some innovations may not be sound business decisions.

There are also physical limitations of the trend toward small. Buttons have become so small that those with large hands may have difficulty pressing only one at a time. Plus, older workers may have difficulty reading button labels—or anything at all—on a tiny screen.

Here's the lesson: When purchasing software, ask the tough questions. Is it really going to improve the way the work gets done, save money, and/or result in the more efficient use of time? When you look at hardware for your staff, always obtain sample devices for them to test and manipulate. Gather feedback, and then listen to their suggestions. It could mean the staff will be more willing to actually use the devices, and this will improve their productivity.

Too Many Choices?

There have been occasions that I'm certain I spent more time setting up the software and hardware to accomplish a

▶

given task than I spent accomplishing the task. A full menu gives you greater flexibility and more choices. A limited menu means faster decisions and less time spent on the task.

In some cases, are we providing our colleagues and employees too many options and too much flexibility? Having too many options may actually make it more difficult to get the job done. Does someone who spends most of his or her time editing text and spreadsheets for intradepartmental communications really need a full copy of Photoshop to accomplish those tasks? A less expensive and more limited program may still have all the tools needed, but without forcing the user to wade through as many complex options.

Lesson: Analyze the tasks you or your staff have to accomplish, and authorize the purchase of software and hardware to meet those needs in the most efficient and direct manner. You may not be able to create an animated GIF file, but those aren't much use on a departmental memo anyway.

The Price of Power

Complex and expensive programs usually require high-priced, powerful hardware. Ever upgrade one of your favorite programs only to find out it won't run on your three-year-old PC or on the current version of your operating system? I recently upgraded my mapping program, which integrates with a certain office suite, only to discover that the new version of my mapping program can't (or won't) talk to that legacy office suite. It's like having two old friends who are angry with each other.

It appears that the interaction of applications will likely only increase in the future, and such surprises will occur more often. Integrated office suites solve part of the problem, as long as you use only the applications that are part of the suite. The issue of backward compatibility also enters the fray at this point. Although my legacy version of a popular office suite meets all my needs, it cannot efficiently open or properly display files created with the latest version of the same program.

Lesson: Purchase your hardware to run your software. You may not need the latest, fastest, hottest gaming machine to run your office suite, but you want to purchase a machine at least one step above what your software requires. You can be certain the upgrade will need more power and space. Also, look for common denominators. If you are sending formatted text files from your machine, will rich text format files carry your formatting? If so, then your older office suite may well be sufficient to work with a colleague's shiny new one.

The Need to Know How

You upgrade one of your favorite programs, then open it up and find a totally unfamiliar interface. The menus look different, and the choices have become so numerous that they don't even show the entire list unless you click a second time to display the whole thing. And when did menu items become so complex we need pictures to understand the functions? Years ago, I used WordPerfect 5.1 on my PC, and all the functions I needed were mapped to the twelve F keys at the top of my AT keyboard. I could fly with that simple interface. Then something "wonderful" happened: With the convenience and flexibility of a windowed interface, and with mouse control, came so many more options that the function keys were outnumbered. I had to relearn how to use my office suite.

With each upgrade to my favorite software come changes that affect the way I use the program. Some changes I learn immediately because I cannot accomplish my daily tasks without those features. Other functions, like a mail merge, for example, come up far less often and require research and lots of questions to otherwise busy colleagues. When you proudly present your employees with a shiny new version of their favorite software package, it is wise to remember that they will likely stumble a bit before running again.

Lesson: Before introducing an upgrade or a new package, research the "What's New in Version X.X" information available on the company website. Try to determine, first of all, if there is anything new in there that you need. If not, consider postponing the upgrade. If you must upgrade, sit down with some staff or colleagues and look at the new version and the list of what's new. Decide whether the interface has changed or the functionality has changed enough to require training. Provide the training or support needed to make the transition smoothly. If you don't, you may notice that, despite the shiny new software, productivity has gone down while your staff struggle in frustration.

Be a Pioneer on the Trailing Edge

A wise young professor once told me that he wanted to be a pioneer on the trailing edge of technology. He meant that he wanted to add important technological features to his courses and to his workplace, but he wanted to use proven technology that could be supported and would be familiar to the majority of his students. He found that the time wasted configuring bleeding-edge technologies with the legacy systems he had available, the time spent learning to integrate the technologies with each other, and the time invested in learning to use and teaching others to use those technologies was too much for the expected return.

There are some advantages to nearly every improvement to the technology that surrounds us. The tablet PC has tremendous promise in situations where one needs to be mobile and record information via a pen-based interface. There are very promising applications in inventory control and the medical profession.

With all the improvements in connectivity and convergence of function so much a focus of our technology efforts, there are some trade-offs that must be carefully considered and factored into the total cost of implementing new hardware and software. A wireless connection is of no additional value to someone whose PC is still sitting in the same place it always has and is not likely to be moved. Newer and faster is not necessarily better, and it always pays, in every way, to make well-informed decisions.

Elwin "Mick" McKellar, Jr., is retired from Michigan Technological University. He can be reached at mick@pasty.net.

▼

Correction to Spring *ACUTA Journal*

In the article "KU Advanced Network Services Registry" in the Spring *ACUTA Journal*, there is an error in the illustration on page 42. The box between the "End-User Device" and the "Access Control Manager" should be labeled "WLAN Access Point." We apologize to the author and to our members if this caused any confusion.

Advertisers' Index

★ **Indicates ACUTA Corporate Affiliate**

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

★ **1Call, A Division of Amtelco** 13, 19
Matt Everly (800/356-9148)
4800 Curtin Dr., McFarland, WI 53558
info@1call.com
www.1call.com

★ **3Com** .... Inside Back Cover
Rick Olivieri (508/323-5000)
350 Campus Dr., Marlborough, MA 01752
rick_olivieri@3com.com
www.3com.com

★ **Campus Televideo** 29
Tony Fell (773/697-6861)
1300 W. Belmont Ave., Ste. 205, Chicago, IL 60657
tfell@camptv.com
www.campustelevideo.com

★ **CommuniTech Services, Inc.** 5
Neal Shact (847/981-1200 x600)
321 Bond St., Elk Grove Village, IL 60007
neal@communitechservices.com
www.communitechservices.com

★ **Compco, Inc.** 7
Randy Burns (615/373-3636 x148)
5120 Virginia Way, Brentwood, TN 37027
rburns@compco.com
www.compco.com

Dees Communications 21
Louis Champan (425/869-1963)
4130 148th Ave. NE., Redmond, WA 98052
sales@dees.com
www.dees.com

★ **Dux Public Relations** 37
Kevin Tanzillo (972/889-9577)
5713 Maidstone, Richardson, TX 75082-4970
kevin@duxpr.com
www.duxpr.com

★ **Fluke Networks** 3
6920 Seaway Blvd., Everett, WA 98203
www.flukenetworks.com

★ **Hubbell Premise Wiring** .... Inside Front Cover
Jo Anne Rush (860/535-5349)
14 Lord's Hill Road, Stonington, CT
jrush@hubbell-premise.com
www.hubbell-premise.com

★ **NEC** .... Outside back cover
Sydney Burton (214/262-2430)
6535 N. State Hwy. 161, Irving, TX 75039
sburton@necunified.com
www.necunifiedsolutions.com

★ **Telecom Technology Resellers** 9
Michael Forst (636/527-7100)
440 Sovereign Ct., St. Louis, MO 63011
mikeforst@teltechresellers.com
www.teltechresellers.com

Western Telematic, Inc. 15
Dave Morrison (949/421-4119)
5 Sterling, Irvine, CA 92618
davem@wti.com
www.wti.com

★ **WTC** 11
Shelley Hasselbrink (213/689-5314)
801 South Grand Ave., Ste. 700, Los Angeles, CA 90017
shasselbrink@wtc-inc.net
www.wtc-inc.net

Zone Telecom, Inc. 25
Tiffany Hancock (888/403-4035)
1125 S. Blackhawk Blvd., Mount Pleasant, UT 84647
thancock@zonetelecom.com
www.zonetelecom.com

Maximize Your Advertising Investmentwith ACUTA

- The *ACUTA Journal* is regularly read by telecom/datacom managers, directors, and others responsible for campus communications technologies.
- When we post the issue to our website (on a one-issue delay), each ad is replaced with the company name and URL.
- Each advertiser is listed by company name with complete contact information in the advertisers' index.
- In the e-mail we send to subscribers alerting them that the *Journal* is in the mail, we list the advertisers and include a link to their website.
- Corporate affiliates who advertise accumulate points in ACUTA's point system.
- ACUTA members notice which vendors support the association.

• • • • • • • • • • • • • • For complete details, contact
Amy Burton, Manager, Corporate Relations & Marketing

Phone: 859/278-3338 x240 • e-mail: aburton@acuta.org
www.acuta.org

continued from page 48

employees, faculty, security, and medical personnel communicate in a crisis without an infrastructure? How would educational delivery be maintained, and what about the safety and security of students, employees, and faculty during a crisis situation? Conducting a risk and security assessment is a critical component in developing a campus BCP/DRP.

A subcomponent of a BCP/DRP is to first conduct a business impact analysis (BIA). A BIA examines the elements of risk in the form of a risk assessment. Risk would consist of three components: asset, threat, and vulnerability.

1. An IT asset or data asset is an item or collection of items that has a quantitative or qualitative value to a college or university. Some common assets are workstations, servers, applications, and voice, video, and data communications equipment as well as research and development intellectual property and grant research information and data.

2. A threat is any agent, condition, or circumstance that could potentially cause harm, loss, damage, or compromise to an IT asset or data asset owned by a college or university. From an IT infrastructure perspective, threats may be categorized as circumstances that can affect the confidentiality, integrity, or availability of the IT asset or data asset in terms of destruction, disclosure, modification, corruption of data, or denial of service. Examples of threats to an IT infrastructure for a campus or university include but are not limited to the following:

- Unauthorized access
- Stolen/lost/damaged/modified data
- Disclosure of confidential information
- Hacker attack
- Virus and malware
- Denial-of-service or distributed denial-of-service attack
- Acts of God, weather, or catastrophic damage

3. Vulnerability deals with any weakness in the IT infrastructure or IT components that may be exploited to allow a threat to destroy, damage, or compromise IT assets.

Weaknesses in the system design are commonly found with software. There is no software or code in existence that does not have bugs, weaknesses, or vulnerabilities, which is why software vendors limit their liability in their software licensing agreements. They simply cannot take on the liability of imperfect software code in their applications. Many vulnerabilities are derived from the various kinds of software that are commonplace within the IT infrastructure—software that can be exploited by perpetrators seeking to threaten a college or university campus.

Examining the assets, risks, and vulnerability of a campus's IT infrastructure helps CIOs and directors make sound business decisions pertaining to what needs to be secured and where funding should be prioritized. With the increase in risks, threats, and vulnerabilities and other exploits in IT infrastructures, IT security professionals are often unable to address known vulnerabilities before the next unknown vulnerability appears. This catch-22 scenario forces IT professionals and management to determine, from a risk- and security-assessment perspective, the most mission-critical assets. Most IT budgets are limited, especially for investments in securing the IT infrastructure. This limitation forces an organization to prioritize funding carefully.

Risk and security assessments allow the organization to assess which IT and data assets must be protected and secured more than others. In addition, a risk assessment will allow an organization to make informed tactical and strategic business decisions pertaining to securing its most valuable IT and data assets.

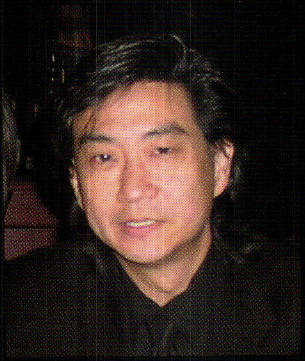
The Human Element

Finally, a risk and security assessment allows an organization to understand the roles, responsibilities, and accountabilities for IT professionals and IT security professionals throughout the organization. Risk and security assessments typically find gaps and voids in the human responsibility and accountability for dealing with risks, threats, and vulnerabilities. Given the magnitude of the IT security responsibility, segregation of duties and dissemination of these duties to IT and IT security professionals is a critical step in many IT organizations in higher education. The dissemination of roles, responsibilities, and accountabilities throughout the IT infrastructure or areas of risk management can be clearly defined once the risks, threats, and vulnerabilities are identified within an organization's IT infrastructure.

David Kim was the chief operating officer of (ISC)^2 Institute, the education and delivery arm of (ISC)^2 (www.isc2.org), the certification and accreditation body of the CISSP® certification for information security professionals. He is currently the president and chief security officer of Security Evolutions Inc. He can be reached at dkim@securityevolutions.com.

▼

Here's My Advice



David Kim
Security Evolutions, Inc.

Risk and Security Assessments for Your Campus IT Infrastructure

Many colleges and universities are now considering performing a risk and security assessment to determine the level of security for their entire IT infrastructure. Such an assessment may indicate that certain steps are necessary to secure the privacy information and data specific to students, employees, and faculty members. This increase in concern, coupled with recent privacy and compliance laws such as FERPA and HIPAA, reflects a general awareness of the importance of maintaining the confidentiality of grades, financial information, and personal healthcare information of students and employees.

Goals and Objectives of a Risk and Security Assessment

There are many goals and objectives that a college or university may consider prior to undergoing a risk and security assessment. Some may be the result of required compliance with new laws, mandates, and regulations for information security.

A sound and comprehensive security process coupled with a robust IT security architecture and framework (e.g., policies, standards, procedures, and guidelines) will help an organization ensure the integrity of its IT infrastructure and assets and meet the organization's minimum acceptable risk or exposure level. This exposure level must be properly aligned with the institution's business liability and asset replacement insurance policy as part of the organization's security process definition. This security process would incorporate three key elements: prevention, detection, and response.

1. Prevention deals with the implementation of security controls and countermeasures or safeguards within the campus IT infrastructure to ensure that the confidentiality, integrity, and availability of the system or application are protected.

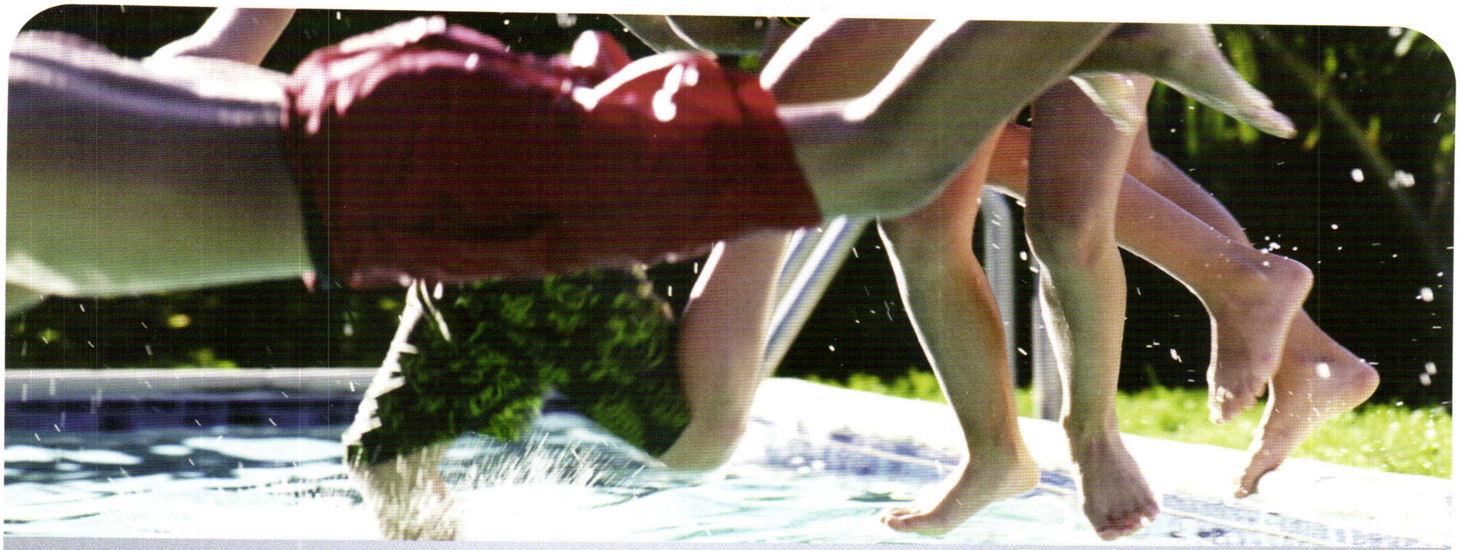
2. Detection focuses on monitoring IT infrastructure and assets, including the use of such tools as log files, audit trails, intrusion detection systems, and vulnerability assessment reports.

3. Response deals with the reaction of the IT organization to a security breach or incident.

Where Does a Risk and Security Assessment Fit in with an Institution's Overall Strategic Plan and IT Infrastructure?

The devastation caused by Hurricane Katrina has motivated many colleges and universities to invest in the development of a comprehensive business continuity plan and a disaster recovery plan (BCP/DRP) for their IT infrastructure. It is apparent that voice, video, and data communications and the infrastructure that supports these services are all critical and essential elements. Most of us can only imagine having no voice or data communications or Internet access. How would key campus

continued on page 47



Last one in is a rotten egg.

Go ahead and get a jump on the 3Com® Summer School savings event. It's your chance to realize exceptional savings on 3Com's Solutions for Education—from networking to wireless to IP Telephony. So why wait? If you're eager to improve your school's performance and enhance your learning environment, now's the time to dive right in.

3Com Summer School 2006

www.3com.com/summerschool/30

3com

security
VoIP
wireless
switching
routing
services

Are you ready for the Digital Generation?

Digital Generation \'di-juh-tuhl je-nuh-'ray-shun\

Definition: 1. a group of contemporaneous individuals with cultural or social characteristics, technological experiences and attitudes. **2.** individuals who see limitless possibilities through the use of technology - to imagine, to dream, to envision new possibilities, to create and of course, to learn!

Today's students have grown up in a digital world along with a sea of electronic digital devices. Naturally, when selecting a school, they expect the latest in cutting-edge technologies to be offered.

Let NEC show you how to meet the communication needs of the Digital Generation. Our solutions for higher education provide a full range of the latest cyber-infrastructure technologies, enabling campuses to offer innovative teaching methodologies, drive new sources of revenue and manage costs. NEC's solutions are comprised of voice, data and video products, applications and services built on the latest IP communication technologies. These solutions address campus needs ranging from mobility to network security and campus safety.

www.necunified.com/highered

Empowered by Innovation NEC