Here’s a thought—to implement Unified Communications and transition to IP on your campus, you don’t have to rip out and replace your legacy systems, taking a big hit on your IT budget. AVST has spent over 25 years developing and delivering a better idea. CallXpress® supports over 250 different PBX/IP-PBXs and Centrex integrations. This has enabled hundreds of leading higher education organizations to build on what they have, implementing Unified Communications and transitioning to IP telephony smoothly and economically with a future-proof solution. To find out more about how you can build onto your existing telephony investment, get our Education Resource CD by visiting www.avst.com/education, or call us at 949.699.2300. We’ll show you why so many well-known colleges and universities like our way of thinking.
<table>
<thead>
<tr>
<th>Event</th>
<th>Date</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spring Seminar</td>
<td>April 6–9, 2008</td>
<td>Sheraton St. Louis City Center&lt;br&gt;St. Louis, Missouri</td>
</tr>
<tr>
<td>Annual Conference</td>
<td>July 13–17, 2008</td>
<td>Caesars Palace&lt;br&gt;Las Vegas, Nevada</td>
</tr>
<tr>
<td>Fall Seminar</td>
<td>October 5–8, 2008</td>
<td>Boston Park Plaza Hotel&lt;br&gt;Boston, Massachusetts</td>
</tr>
<tr>
<td>Winter Seminar</td>
<td>January 11–14, 2009</td>
<td>Renaissance Esmeralda Resort&lt;br&gt;Palm Springs, California</td>
</tr>
</tbody>
</table>

**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

FEATURES

10
Disasters, Emergencies, and Residence Hall Communications
Geoff Tritsch & Michael Grunder
Tritsch and Grunder suggest some sound safety reasons for providing at least a minimum number of wired phones in residence halls.

16
GWU’s Safety Systems Built Around Telecommunications
Jennifer Paire & Curt Harler
George Washington University won top honors recently for its campus safety and security program. Find out what makes their plan stand out in this article.

20
In the Face of Disaster
Mick McKellar
From the experts, McKellar presents the hallmarks of good emergency planning, then discusses how three campuses fared when they met disaster face to face.

24
Advertorial: Contact 101: Strategies for Emergency Notification
Bill Grabner
Both push and pull technologies are vital to effective emergency notification. Grabner of Genesys describes how their products meet the needs of today’s campus.

28
University Approaches to Emergencies and Emergency Communication
Ron Kovac, PhD
Kovac presents some of the features common to emergency plans submitted to ACUTA by various campuses. Compare your plan to this analysis of others’ plans and be better prepared.

31
A Reasoned Response to Crisis
James Satterfield
Against the background of the tragic shootings at Virginia Tech, Satterfield advises predict, plan, and perform. This article also shares some of the lessons learned from this event.

33
Digital Forensics: What Is It and Why Should I Care?
Ron Kovac, PhD
More and more frequently, computers and networks are used in criminal activity. Tracking down the perpetrators often requires following an elusive trail. Learn more about the footprints that digital forensics seeks to identify and follow in criminal investigations.

38
Exploits, Guidelines, and Vulnerabilities: Protecting Digital Resources
James S. Cross, PhD & Steven Samaras, PhD
Protecting digital resources is a critical (and expensive) undertaking. Cross and Samaras raise some interesting questions about how information is threatened as well as how it can be protected.

42
Classifying Events, Incidents and Disasters
Marjorie Windelberg, PhD
Classifying incidents makes planning a response to a disaster or emergency on campus more effective. Windelberg suggests a format for identifying and assessing risk and creating a plan to mitigate the impact of any event.

COLUMNS

6
President’s Message
Walt Magnussen, PhD, Texas A&M University

8
From the Executive Director
Jeri A. Semer, CAE

48
Here’s My Advice
Janet Smith

ADVERTISERS’ INDEX

46
Thanks to the companies that support ACUTA by advertising in our Journal.
inCampusAlert

TAKE A PAGE FROM OUR BOOK. LEARN HOW TO NOTIFY THOUSANDS OF STUDENTS IN SECONDS.

THE BEST NOTIFICATION SYSTEM FOR TWO-WAY COMMUNICATION FOR DAILY CAMPUS EVENTS, EMERGENCIES, SURVEYS, IT-RELATED ALERTS, AND FIRST RESPONDER MOBILIZATION

Built on the MIR3™ Intelligent Notification platform used by the largest corporations, inCampusAlert is a fully featured emergency notification system designed for and selected by colleges and universities of all sizes.

INCOMPUS ALERT — USED BY OVER 120 COLLEGES AND UNIVERSITIES FOR ALL THE RIGHT REASONS

- Fast Deployment — inCampusAlert can be implemented in hours, not days.
- Ease of Administration — Colleges can import data directly, synchronize database with the system or students can self-administer.
- Variable Architecture — Whether it is one campus, a multitude of satellite campuses, or a state wide organization, inCampusAlert’s support for groups, departments and organizations is flexible to enable compliance to existing structure.
- Multi-Modal Communications — inCampusAlert delivers recorded voice, text or text-to-speech messages to every communication device or service including cell and satellite phone, landline, PDA, email, pager, fax, and conference bridging.
- 24/7/365 Support — inCampusAlert is backed by a Support Center staffed around-the-clock by highly trained technical experts to ensure readiness no matter when an event occurs.
- Fixed Cost — MIR3 understands the stringent fiscal constraints colleges face and offers a price structure that provides a premiere service at a fixed cost.

LEARN DIRECTLY FROM THE COMPANY THAT WROTE THE BOOK ABOUT EMERGENCY NOTIFICATION.

download today: white paper
Understanding Notification Modalities - The Key Requirements - www.mir3.com/wpnm

©2008 MIR3 Inc. All rights reserved
The only way to recover from such disasters is through advance planning and consideration of all possible scenarios, from floods to fire, from hackers to hurricanes, and from tornadoes to terrorism.

Mick McKellar

4

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, Membership Marketing & Corporate Relations
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 institutions or companies. ACUTA, as an association, does not express an opinion or endorse products or services.

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

Contents of this issue of The ACUTA Journal are copyrighted: ©2008, ACUTA, Lexington, Kentucky.
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 Michele West, Membership Services Manager, 859/278-3338, ext. 222, or e-mail mwest@acuta.org.

ACUTA
2007-2008 Board of Directors
President
Walt Magnussen, PhD, Texas A&M University
President-Elect
Corinne Hoch, Columbia University
Secretary/Treasurer
Rini Ledgerwood, San Diego State University
Immediate Past President
Carmine Piscopo, RCDD, Providence College
Directors-at-Large
Harvey "Buck" Buchanan, Florida State University
James S. Cross, PhD, Longwood University
Randal J. Hayes, University of Northern Iowa
Diane McNamara, Union College
Sandra Roberts, Wellesley College

Publications Committee
Ron Kovac, PhD, Ball State University, Chair
Lee Badman, Syracuse University
William A. Brichta, Delaware Valley College
Janice Bundy, University of California, Los Angeles
Gary Coleman, Verizon Business
Peggy Fischel, Middlebury College
Les Shaw, University of Maine
Dave Wirth, Princeton University
Ex Officio
Walt Magnussen, PhD, Texas A&M University
Jeri Semer, CAE, ACUTA Executive Director
Board Liaison
James S. Cross, PhD, Longwood University
Staff Liaison
Pat Scott, ACUTA Communications Manager

Editorial Review Board
Dave Barta, University of Oregon
Tamara Closs, Duke University
James S. Cross, PhD, Longwood University
Jay Gillette, PhD, Ball State University
Mike Grunden, Vantage Technology Consulting Group
Ray Horak, The Comnet Corporation
Jeanne Jansenius, University of the South
Patricia Todas, Northwestern University
Michael Williamson, Springfield College
Solutions for higher education professionals

Ask a higher education professional why they love their BlackBerry

You have a lot going on — and BlackBerry® smartphones have the features you need. BlackBerry smartphones are designed to make it easy to stay in touch with people and events that matter to you. With BlackBerry smartphones, you can: browse the web and conduct research; email a colleague or an entire class; send a voice note to your assistant; organize appointments and reminders on the spot; and with the ability to access your data over almost any WiFi network** in addition to your cellular network, you can maximize your productive time and help minimize costs, from almost anywhere you are. Is it any wonder why so many of the smartest people around love their BlackBerry smartphone?

- Collaborate, conduct research and organize — while on the go
- Stay in touch effortlessly by email, phone or voice notes
- Built-in Global Positioning System (GPS) with BlackBerry® Maps allows you to map out geographic locations and view turn-by-turn driving directions***
- Keep on top of your research, lectures and appointments with an easy-to-use, intuitive user interface

Discover special offers for education professionals at www.blackberry.com/faculty

**Check with service provider for roaming arrangements, service plans and supported features and services. Voice note feature requires BlackBerry® Device Software version 4.60 or later. ***GPS feature requires version 4.2.1 or higher of BlackBerry® Device Software for CDMA smartphones and 3.6x or higher for CDMA/EDGE smartphones.

Research in Motion Limited. All Rights Reserved. The BlackBerry and RIM family of related marks, images and symbols are the exclusive properties of Research In Motion Limited. RIM, Research In Motion, BlackBerry, "Always On, Always Connected" and the "e-smartphone in motion" symbol are registered with the U.S. Patent and Trademark Office and may be pending or registered in other countries. All other brands, product names, company names, trademarks and service marks are the properties of their respective owners. Screen images are simulated.
How Technology Steps Up to the Challenge

This issue of the ACUTA Journal is dedicated to Preparing for Disasters and Emergencies, and it would be hard to pick a more appropriate topic. There is actually good news as well as bad news in this space. The bad news is that the frequency and severity of incidents seem to be on the rise. The good news is that the technology that we all work with is creating interesting opportunities for us to protect ourselves.

The fact that the number of incidents is on the rise can be validated by looking at Carnegie Mellon’s Computer Emergency Response Team (CERT) statistic page (http://www.cert.org). They recorded 137,529 incident reports in 2003. This was three times the number of incidents reported in 2001 (52,658) and more than ten times the number of reported incidents in 1999 (9,859). It can also be seen in natural emergencies. According to NOAA statistics (http://www.noaa.gov), 2004 and 2005 were two record-setting years with 28 named storms (2005), 15 hurricanes (2005), nine U.S.A. landfalling named storms (2004), and four U.S.A. landfalling major hurricanes (2005). All of this activity has been putting major strain on campus resources.

On the positive side, technology has been stepping up to the plate by providing resources that help us mitigate these vulnerabilities. The technologies that have proven to be the most valuable can be found in fiber-supported voice and wireless services.

The first major enhancement was provided by the carrier’s high-speed optical networks and by university-owned and -run regional optical networks (RONs). This service now allows us to provide high-speed, reliable, offsite machine-room space at a reasonable cost. In the past, we were required to house all of our critical applications in one (or two if we were lucky) central machine rooms. With the advent of high-speed optics, we can now extend our machine rooms into either the university’s machine room or leased space from a high-reliability commercial data center.

The second way that technology has stepped up to the challenge comes from the inherent architecture of VoIP. The older TDM architectures typically involved one large, central switching platform, which was difficult to distribute. (Many platforms allow for the distribution of switching nodes but they still require the presence of the central switching system). VoIP architecture allows the presence of multiple servers that can be easily distributed across several locations. In a VoIP network, the loss of any single geographic location can fairly easily be routed around. In addition, VoIP also allows for the blasting of thousands of simultaneous calls for alarming, which is either difficult or impossible in most TDM architectures.

The third area in which technology has changed the way that we support emergency services is student and faculty/staff notification. For at least a decade, my campus sought a way to notify our 45,000 students in the event of a crisis. We had looked at siren systems, email trees, and classroom alarm systems and had found them all to be either ineffective in our case or cost prohibitive. With the invention of SMS text messaging, the students brought a reasonable solution to us.

I am sure that there are several other ways in which technological advances have helped us deal with the ever-increasing threats that are the reality of today’s world. Fortunately, ACUTA has been on the leading edge of all of these advances by having our institutions share successes (and failures) with others. At the last two seminars, there were several sessions on emergency notification. In Minneapolis the FBI shared their efforts with us, and last summer, ACUTA had a webinar covering this topic. Since the level of threat does not seem to be going away, I personally feel better knowing that my campus is not alone in the battle.
With Nextel Direct Connect,® only from Sprint, you’re prepared to avert an added emergency in an emergency. Nextel Priority Connect helps you reach the right people instantly, without fighting a clogged system. And Nextel Direct Connect phones can offer interoperability with land mobile radios, allowing you to connect faster to more teams nationwide. When seconds count, you can count on the world’s largest and fastest push-to-talk network. That’s getting it done at SprintSpeed.™

In partnership with America’s Most Wanted, Sprint is the proud sponsor of the All-Star Challenge. Go to sprint.com/government to submit your nominees.

1-800-SPRINT-1
sprint.com/government

When you call for backup, Nextel Direct Connect® has got your back.

Speed claim based on initial call set-up times. Nextel National Network reaches 274 million people. Network coverage not available everywhere. Other restrictions may apply. ©2008 Sprint. Sprint, the logo and Nextel Direct
Connect are trademarks of Sprint.
Many institutions have taken steps during the last two years to implement, review, and update their emergency notification systems. A series of major hurricanes, fires, violent incidents, and other disasters on college and university campuses in recent years have brought heightened attention to the need, and advances in technology have made it more feasible to implement systems using broadcast voice, text, and e-mail as important components of disaster preparedness.

One of the issues that institutions need to be aware of when designing these systems is the legal and regulatory framework within which they operate. In the United States, these include laws related to telemarketing, broadcasting recorded messages to landlines and cell phones, and spam. State laws and regulations may also apply, and these do vary. We recommend that you check with the institution's legal counsel or your state's regulatory agencies regarding state requirements.

We asked ACUTA's legal counsel, Wiley Rein LLP, to investigate this matter and advise us as to the federal statutes and regulations that apply to emergency notification—whether broadcast by the non-profit institution internally or a third-party agent. The following summarizes counsel's findings by type of activity. Links to the pertinent laws and/or regulations are available on the ACUTA website at http://www.acuta.org/index.cfm?1991. (You will need a My ACUTA account to view this document.)

**Telephone Calls (live or recorded) and Text Messages Sent to a Phone Number**

The rules of the Federal Communications Commission (FCC) adopted pursuant to the Telephone Consumer Protection Act (TCPA) permit a live or prerecorded telephone call to a phone number, if made for "emergency purposes." Neither prior express consent nor an established business relationship is necessary in order to legally make these communications.

The TCPA and FCC rules that were adopted to implement this law clearly state that calls made for emergency purposes are exempt from the prohibition on using automated equipment to make either live or pre-recorded calls. These calls must not contain commercial or advertising content.

FCC rules also explicitly exempt emergency calls that are "made by or on behalf of a tax-exempt nonprofit organization." This section would clearly apply to a situation in which the institution has outsourced the notification process.

In addition, the telemarketing rules of the Federal Trade Commission do not apply to emergency communications by colleges or universities if they do not contain an inducement to purchase goods or services or make a charitable contribution.

**E-Mail or Text Messages Sent to an Internet Address**

Colleges and universities may send emergency text messages via the Internet without violating the CAN-SPAM Act or FCC rules. The FCC's CAN-SPAM rules only apply to commercial text messages sent to an address that includes an Internet domain name. A commercial message is "an electronic message for which the primary purpose is commercial advertisement [or promotion]." Thus, emergency messages that lack a commercial component and that are sent via the Internet by an institu-
tion or its agent fall outside the scope of the CAN-SPAM rules.

Outsourced Solutions Using Third-Party Agents

Several institutional and corporate affiliate members have inquired about how these regulations apply to for-profit companies that host emergency notification systems for colleges or universities. Companies hired by colleges and universities want to ensure that they are complying with all of the applicable requirements, and they are legitimately concerned that they may be required by law to obtain opt-in permission before sending voice or text messages or e-mails.

ACUTA's legal counsel posed this question in January 2008 to an attorney with the FCC's Consumer and Governmental Affairs Bureau who is responsible for working on TCPA matters. This FCC official confirmed that colleges and/or their agents can send text messages without the recipient's prior express consent, if the messages exclusively contain emergency communications and are not commercial in nature.

Whether the entity sending the messages is for-profit or non-profit does not affect this analysis—the key point is that the message exclusively contains emergency communications. Our legal counsel advises that this applies to voice or text messages sent to phone numbers, emails, and text messages sent to phone numbers containing an Internet domain name.

For these reasons, a for-profit company that sends emergency communications on behalf of a college or university without the recipients' prior express consent does not violate either the TCPA or the CAN-SPAM Act, provided that the messages do not contain any commercial content.

I hope that this clarifies some important issues about the legal and regulatory framework for emergency notification systems. Reach Jeri Semer at jsemer@acuta.org.

Consulting In Telecommunications, Networks, & Information Technology In Higher Education

Experience since 1983

Phillip Beidelman
213-622-4444
www.wtc-inc.net
wtc@wtc-inc.net

Experience
Disasters, Emergencies, and Residence Hall Communications

Geoffrey Tritsch and Michael Grunder
Vantage Technology Consulting Group

Of all the purposes associated with telephones in residence halls, the issue of personal safety is cited as being highest on the list.1 But just how valuable are residence hall phones in an emergency? With falling numbers of students using the wired phone lines in dorms and housing departments under pressure to control dorm costs, wired phone services are an increasingly popular target for removal. This is fueled by a perception by many that the wired phone service in residence halls is hardly used anymore. While this may be true in some cases, survey evidence indicates that it is not the case in all situations. Issues such as cellular coverage, local calling area included in the base rate, whether sets are provided, whether long distance is included, percentage of international students, and many other factors can all affect how much wired lines are used.

The decision to remove wireline residence hall phone service to the rooms must be carefully considered. One important aspect of this decision is the role of residence hall wired telephone service in case of emergencies.

Background

It is important to appreciate that the entire student resale situation, which in turn led to providing telephone service in the residence halls, was an anomaly—a onetime window that happened as we made the transition from a regulated to a competitive environment. There were opportunities based on the disparity between individual residential long-distance rates and the volume discounts that early resellers could get. Colleges and universities were ideally positioned to be first-in with a captive customer base and in-place or easily installed infrastructure. Additionally, colleges and universities had freedom from the regulatory restrictions that commercial resellers had to face. We all have had to come to terms with the fact that this opportunity (which served us well for almost 10 years) will not happen again (at least not to the same extent). But it was student resale that produced both the need (desire?) for phones in residence halls and the funding to accomplish it.

Colleges and universities use various models for providing residence hall telephone service. Some institutions provide a line per room and some per pillow; some provide a line bundled in the room rate and some provide it optionally or as a separate fee; some provide it with a telephone set and some without. Of these, the most common model is a telephone line provided per room with the telephone set to be provided by the student. In many early scenarios sets were provided by the institution. However, the hassles associated with set provisioning, placement, tracking, and repair drove many institutions to the student-provided set model. Of all the models for providing residence hall phone service, this—the most popular model—is also the least useful from an emergency communications standpoint.

One more point before we begin to explore that last, somewhat inflammatory, statement. Even though "public safety" and "liability" are often cited as intermingled reasons for keeping wired residence hall phone service, there is a significant difference between them. Liability is inwardly focused, looking at protecting the institution's finances and reputation should an incident occur. Public safety is outwardly focused, looking at protecting the campus community from incidents and/or mitigating the results should they occur.
MASS NOTIFICATION PAGING EMERGENCY COMMUNICATION

WEBS™

BY TALK-A-PHONE

At Talk-A-Phone, we have developed technologies that have made us good listeners and talkers. With WEBS, we have given you the ability in an emergency situation, to broadcast security over a wide area. WEBS™ (Wide-area Emergency Broadcasting System) can be heard 1000 ft in every direction. All call paging, zone paging, or single location paging. Wired or wireless. Integrated emergency phone. Listening is a skill but sometimes it's good to be loud, really loud.

WEBS® & Talk-A-Phone are registered trademarks of Talk-A-Phone Co. *Patent pending

TALK A PHONE
Creating Communications Solutions

5013 NORTH KEDZIE AVENUE CHICAGO, IL 60625 U.S.A.
TELEPHONE 773-539-1100 FAX 773-539-1241
WWW.TALKAPHONE.COM INFO@TALKAPHONE.COM
There are two aspects of emergency communications: outbound—the student getting assistance should something occur, and inbound—getting word to the student in case of an emergency.

**Outbound Emergency Calling**

Personal safety, including the ability to call for help, tops everyone’s priority list (or it did before emergency notification became foremost in everyone’s mind). While it is comforting to think that help is just a phone call away, the most popular residence phone model may be the least useful. While it may address liability, it does not address public safety. Telephone lines without telephone sets attached to them are of little use, especially in an emergency! Many institutions report that a very limited number of students use dorm phones or even bring a telephone set to use. That pretty much leaves cell phones as the way that most students will call for assistance.

Cell phone programs affiliated with or provided by the institution are increasingly popular as are no-phone programs that rely on the students to provide their own cell phones, but cell phones are not without their problems. These include, but are not limited to, coverage, reliability, and 911 issues. Distributed antenna systems and more local cell towers may address the coverage and reliability issues (assuming they can be cost-effectively provided) but not the 911 issues.

Most people are familiar with 911 and efforts to establish a uniform nationwide emergency number. Enhanced 911 (E911) adds to this by automatically reporting the location of the caller. This is of obvious importance when the callers are unable to report their location themselves. Deployment of 911 started more than 30 years ago and is still incomplete, believe it or not. While most colleges and universities have some form of 911, there is no single, uniform model. Some institutions are their own public safety answering points (PSAPs); some rely on the city, county, or state PSAP exclusively; some handle calls jointly with the public PSAP; and some prefer that campus police answer the call first and only involve the public PSAP if needed. Many institutions still use an on-campus, non-911 number for campus police and differentiate between 911 (public emergencies) and campus emergencies. No matter how 911 is handled, it is an important aspect of campus safety.

While E911 should not be the only driver in selecting a student telephone service, it is a factor that must be considered. Any decisions on 911 should be made by commission, not omission. While cell phones (and VoIP) are both viable solutions for student services and are increasing in popularity, both of these technologies present challenges to 911 officials. The databases that provide the location information are not able to cope with new technologies and the increasing degree of mobility they provide.

The 911 issues with cellular include:

* Not all emergency calls go to 911 (other examples include *77, *2222, *SP)
* Limited, if any, location information provided with the call
* Routing the call to the correct PSAP (campus police versus city/county/state)
* Signal strength/coverage
* Occasional failure to connect
* Frequent false 911 calls caused by having 911 on speed dial inadvertently activated in a pocket or purse
* Changing cellular technology

Although the FCC has established requirements for cellular E911 location, none of the solutions is as accurate, reliable, or easy to administer as traditional 911 on wireline telephones. The FCC requires that location information be accurate to within 50 meters 67 percent of the time and 150 meters 95 percent of the time. This approach may be acceptable if someone needs to be located on the football field or along the highway, but trying to get accurate E911 services in dorms will require that we revisit E911 and make some hard decisions about how important it really is.

FCC requirements for triangulation are complex and do not require the accuracy required for residence hall applications. For example, with cell phones, there are four different approaches for approximating the location of a caller. Three of these approaches rely on triangulation and one on GPS. Two of the triangulation approaches require that the caller’s signal be received by at least two towers, and the third approach requires three towers. Cellular coverage in many residence halls is barely even adequate, much less covered by multiple towers—and GPS doesn’t work indoors. In addition, 50 meters (the most accurate FCC requirement for location of a cell phone caller) represents a sphere 100 feet in diameter. In a high-rise dorm this covers 30 floors vertically (+/- 15 floors) and 15–20 rooms horizontally. Thus far the major cell phone providers have consistently failed to meet FCC requirements. This is further complicated by the fact that fewer than 10 percent of the public safety answering points (PSAPs) in the United States are ready to accept this type of location information. E911 is great, but cellular E911 still has a ways to go.

There are similar issues with VoIP. The fact that an IP phone can be easily relocated to any voice-ready port on the data network creates complexities for E911. These include:

* Identifying the physical location from which an emergency call originates
* Identifying the right PSAP as an IP phone could be located anywhere and not necessarily in the same system, exchange, area code, or even the same country
* Associating emergency line identification number (ELIN) with location

With VoIP there is a work-around using ELINs that can provide static location information to a phone or group of phones.
While this works well in an office environment (especially in an open office landscape design), it does not provide the level of accuracy required for closed dorm rooms. With ELINs it is easy to provide location information for an entire residence hall or even a floor but to identify a single room would require an additional DID number to act as the ELIN for every room! (This is not an issue if the VoIP phone service is provided through an IP-analog gateway as the analog lines are not mobile the way that the pure IP lines are.)

It is clear from all this that some wired phones should remain in dormitories. If an institution were to remove all wired phones from student rooms, we recommend that public access phones in the hallways and phones in resident adviser rooms should be provided both as a backup and a means of emergency communications.

Inbound Emergency Calling

As far as emergency notification is concerned (i.e., quickly alerting the entire student population of an emergency), residence hall wired phones may be the worst possible option. Inactivated lines and lines without sets are obviously useless. Even if all lines are active and have phones, out-calling to dorm phones can be relatively slow and has a potentially low call completion rate. If students are in their dorm rooms, sirens, fire alarms, and public address announcements can all be more effective (but perhaps less detailed) means of communication. If the students are not in the dorms (very likely), text messaging and calls to cell phones are better choices.

We recommend that critical messages should be sent out over multiple media simultaneously via telephone call/voicemail, SMS text message, e-mail, manual “phone trees,” streaming video, and as a trailer message scrolling across the bottom of every CATV channel. None of these communication methods, however, will guarantee the receipt of the message by everyone, although word-of-mouth communication will occur and is effective.

A rather large number of vendors provide emergency notification systems. These are systems that have the ability to alert very large numbers of people, via several communications modalities very quickly (voice calls, text message, email, etc.). These types of systems can be very effective and can play a key role in emergency planning.
and response. Like most things, however, the devil resides in the details and projects concerning these systems require close and detailed planning in the procurement process as well as in implementation, testing, and ongoing usage. As with any recently popularized technology, there are growing numbers of stories regarding bad choices and poor implementations of emergency notification systems.

Liability

Liability is difficult to predict and is often a matter for the courts to decide. Clearly, anything that an institution does that could be construed as impeding the speed of emergency response could become the basis of a liability lawsuit.

Under the legal definition of liability an act (or inaction) must satisfy four basic elements:
1. There must be a legal duty to care for another person;
2. There must be a breach of that duty;
3. Claimant must have suffered damages;
4. Damages must have been proximately caused by the breach of duty.

Looking at these four elements:
1. An institution clearly has some responsibility for students who live on campus in on-campus housing;
2. The removal of room phones might be construed as a breach of that duty;
3. Especially if the claimant suffered damages; and
4. The removal of the phones from student rooms could be shown as having impeded emergency response, such as if the student is unable to get to a hall phone or if the student’s cell phone does not have adequate coverage and is the only means of emergency communications.

When we talked with a personal injury attorney in Massachusetts regarding this topic, he noted that if it could be shown that there was a causal relationship between removing the phones and a delay in emergency services response, the lawsuit would be, in his terms, “a sure thing” for the claimant.

On the other hand, an attorney from the state of Washington indicated that absent any legal obligation by state statute or local ordinance for the institution to provide telephones in the rooms, the situation is a contractual issue. Liability would be based on the reasonable expectations of the parents and students to expect phone service, and that expectation could be set by the housing contract making it clear to all parties that: (1) the institution does not provide room telephones, (2) students are encouraged to have cell phones, (3) cell phones are not guaranteed by the University to work in all applications, and (4) campus public safety should be contacted on a specific phone number.

To what extent replacing dormitory room phones with hall phones might mitigate the liability is unclear and, to our knowledge, yet to be tested in case law, and neither has the extent of the institution’s responsibility associated with cell phones versus wired phones. As one lawyer from California noted, “The law has not caught up with the changes in technology.” We suggest that before any action is taken to remove or even change telephone services in residence halls, the matter should be reviewed by risk management, campus security, and legal counsel.

Conclusion

With the nation’s increased focus on security, parents have heightened concerns for their students’ safety. Reducing costs by removing existing telephone service has to be done with care and only with the buy-in of other college/university departments such as housing, residential life, campus security, risk management, and legal counsel. This is not a decision that should be made exclusively by any single department.

The underlying message here is that the changes in how students use residence hall telephones are only a representation of the greater and more far-reaching issue—how students communicate. The telephone is the first of a number of technology shifts that we will be seeing in the future.

Why don’t students use landlines? Wired phones are restrictive and “so yesterday.” Why don’t students set up their voicemail boxes? VM is not a priority. It is non-real time and not as immediate as IM or text messaging. Why do so many students ignore the institution’s e-mail service? They’ve had email for years now. Why change?

Colleges and universities need to look at student services in a broader context, in the long term, and in an entirely new light. This means getting a group together to examine the entire issue. Telecom, IT, residential life, campus security, legal counsel, and academic administrators must all be part of the process. Sharing information through organizations like ACUTA is highly recommended, but what works for one school may not be the right solution for another. Public versus private, location, size, campus layout, financial resources, and many other factors play a part. This is not just a telecom issue. This is an institutional issue to which telecom holds some of the answers. It is also, once again, an opportunity for telecom to play a leading role in a significant institutional decision.

Geoff Tritsch and Mike Grunder are vice presidents at Vantage Technology Consulting Group. Both have years of experience working with campus technology, and both have been active in ACUTA for decades. Reach Geoff at geoffrey.tritsch@vantagetcg.com. Reach Mike at michael.grunder@vantagetcg.com.

Notes
1. Based on a survey of 14 state universities conducted by Geoff Tritsch in 2006.
2. Vantage is providing information on this topic based on an anecdotal and experiential basis only.

Nothing in this report should be taken as constituting legal advice. Consult legal counsel.
Notifying your personnel, staff and students is as easy as...

Trigger Alert
(click)

RELAX ... the responders are on their way!

Notify Thousands in Seconds with RED ALERT!

Ideal for:
- Campus Lockdowns
- Staff Shortages
- Meeting Reminders
- Scheduled (and Unscheduled) Events
- Network Outages
- Emergencies
- Evacuations
- Weather Emergencies
- Student Safety
- And more!

You’ll find uses for RED ALERT in every department!

Also available from 1Call:

Infinity PC-based PBX Console and Call Center System – Provides highly efficient single-keystroke operator functionality, and enterprise-wide or worldwide access to valuable information and applications.

“Just Say It” Speech Recognition – Automates incoming and dial “0” calls without live operator assistance for a rapid return on investment.

www.1call.com/acuta • info@1call.com • (800)356-9148
(608)838-4194 • 4800 Curtin Drive • McFarland, WI
GWU's Safety Systems Built Around Telecommunications

The ingredients that comprise emergency response systems at George Washington University in Washington, D.C., can be described by the slogan for Prego Italian sauces: “It's in there.” That’s according to John Petrie, assistant vice president for public safety and emergency management at GWU, which is the largest institution of higher education in the nation’s capital.

“Trying to pick out the most important thing just doesn’t work. That’s because it depends on how you’re preparing and what you’re responding to … but nothing can survive without communications except by accident,” says Petrie. “So, we’ve tried to give ourselves options, including redundancy.”

The grid of security at the institution is so thorough it was awarded the International Association of Emergency Managers’ (www.IAEM.org) prestigious Business and Industry Preparedness Award in November for excellence anticipating multiple hazards cost-effectively and linking all levels of the organization at GWU and surrounding emergency response and management agencies.

“The way we approach our planning is to use an all-hazards approach,” Petrie says. “It means we are trying to prepare ourselves for any disruption. It doesn’t matter what has caused it.”

Redundant Telecommunications and Data

GWU has the benefit of being on the same power grid as the White House, so power restoration and maintenance are high priority. Power lines are underground and not as vulnerable to weather.

GWU was able to purchase a data center across the street from its Virginia campus and then replicate it. The other two campuses, at Mount Vernon and Foggy Bottom, are linked to the Virginia location with dark loops and interconnected hub sites. The university has its own telephone system backed up by contractors, and it makes smart use of the Internet. Any interruptions have been limited to a maximum outage of five minutes because the school is backed by four ISPs. Each of the four ISPs also has a system of backup servers protecting its location.

“We also go to tremendous trouble with our records,” Petrie says. “They are backed up electronically in two different locations whenever saved, then downloaded daily and stored in a fireproof room. Then, once a week, everything is taken to an off-site location.”

Making the Most of Everything

One reason the program at GWU has garnered so much respect, even beyond the university community, is its smart use of existing resources within the university and its ability to interact with surrounding organizations. All of GWU’s several campuses are covered by the emergency system. The school maintains a recorded information line (202/994-5050) and a website (http://campusadvisories.gwu.edu), used to inform individuals of incidents that may affect the Foggy Bottom, Mount Vernon, or Virginia campuses.

The university also has a partnership with the District of Columbia to use Alert DC, a system that provides immediate text notification to e-mail, cell phone, and other electronic devices during a crisis or emergency.

“If I send a text message using Alert DC, I can get that out to thousands of addresses in
EXCELLENT QUALITY, COMPETITIVE PRICE, FAST DELIVERY
Hyperline Systems 2212 Gladwin Crescent, unit C7, Ottawa, Ontario, K1B 5N1, Canada
Phone: 1-613-736-8500, toll-free: 1-866-63-HYPER (1-866-634-9737), fax: 1-613-736-9752
www.hyperline.com
just minutes,” Petrie says. “Mobile phone providers determine the importance of delivery. But most will. It’s a very valuable system, but it doesn’t solve the whole problem.”

GW Alert, an immediate personal notification tool for computers using a Microsoft Windows operating system, is available as an emergency notification tool, too. It is the result of cooperation among several university departments and the students.

They’ve dealt with the question of what’s an alarm and what is background noise. The GW Alert never will be mistaken for background noise. “We only use it for emergency management and it has an audible alarm—if you heard this alarm, you would not be confused about whether it was an alarm or not,” Petrie says. “It’s followed by a red crawler that goes across the bottom of their screen … We feel that’s our fastest way to reach people. It’s going on all university-owned computers and was available to students the first of November [2007].”

The public address system makes use of existing police and transportation vehicles. It’s not a first response, but could be deployed during an incident, and it is tested from time to time.

Campus Inconsistencies

Philip Jan Rothstein, FBCI, of Brookfield, Connecticut, is president of Rothstein Associates, Inc. (http://rothstein.com/), a management consultancy and publisher of many books on emergency management. He says that like businesses, the organization of campus emergency management plans across the country varies.

“Some campuses do a great job, some don’t,” says Rothstein, who has consulting services for campus security organizations. “You’re dealing with an immature population. You can deliver information [to students] and it doesn’t always register as it might with an adult.”

Rothstein, who has focused on emergency management for 25 years, believes many schools aren’t designed for safety; nor have they stopped to make plans for it.

“I’m not sure it’s as much a matter of technology as people knowing what needs to be done,” Rothstein says.

IT and Other Professionals Involved

GWU realized early on that running an effective system is like peeling an onion: There are many layers of organizations to deal with. GWU’s planners know they must also hold hands with emergency responders and agencies locally, and Petrie says they are all on the same page.

GWU’s System a Model for Other Industries

George Washington University won the International Association of Emergency Managers’ (www.IAEM.org) prestigious Business and Industry Preparedness Award in November 2007 for its excellence in implementing a program that plans for multiple hazards, sets implementation priorities, is cost effective, links all levels of the organization, and coordinates with local emergency response and management agencies. GWU’s Office of Public Safety and Emergency Management for its Emergency Preparedness Exercise Program accepted the award announced at IAEM’s meeting in Reno, Nevada.

“The purpose of the award is to recognize people and institutions that have done something commendable on emergency management preparedness,” says Larry J. Gispert, president of the IAEM board of directors. He is with Hillsborough County, Florida’s Emergency Management team in Tampa, where he is the county’s director of emergency management.

The IAEM is a nonprofit educational organization dedicated to promoting the goals of saving lives and protecting property during emergencies and disasters. IAEM consists of more than 4,000 emergency management professionals from local, state, and federal governments, the military, private industry, and volunteer organizations. Gispert says they have membership in 45 countries, although most members are U.S. based.

“IAEM has consistently promoted the goals of saving lives and protecting property during emergencies and disasters,” he says. The group was founded in 1952 as the U.S. Civil Defense Council.

It is important to note that GWU was honored in a class that focuses not just on colleges or the educational and public arena, but is a cross-business award. One of the key facts IAEM looks at is whether the program is repeatable by similar organizations in business and industry. In short, IAEM held GWU up as a model for planning, not just for the university community but for all planners.

A big part of the reason GWU won the IAEM award was the fact that the plan is broad-based. “Our organization is trying to perpetuate the need for citizens to be prepared. If we can get citizens prepared, we can lessen their needs when a disaster happens,” Gispert says.

Both colleges and organizations can learn lessons from those events. That’s the reason the Emergency Managers Association recognizes outstanding efforts like GWU’s program.
"The teams we work with use the same philosophies we—they have Sprint-Nextel BlackBerries that have redundant communications capabilities and the antenna systems that provide our coverage with overlapping footprints and their own emergency power. The BlackBerries have direct voice, text, and messaging by radio circuits, so if there's an overload in the cell system, we can still communicate with each other."

The university's text-to-voice system can also employ a conferencing bridge. And a 24-hour recorded voice line is backed up to switch to another code if something happens. That way, recorded calls continue and are limited to 30 seconds so they reach the maximum number of individuals.

Coverage is not limited to recordings. Calling the general line during an incident will reach a real person. The campus has multiple locations for operators, and their systems are backed up.

Community Connections

"We recognize we can't get it all done ourselves," Petrie says. "We have relationships with other institutions, and have a mutual aid agreement with Georgetown University and American University. We have a leadership role in Foggy Bottom and its neighborhood planning committee." In fact, they make it a point to have relationships with their commercial neighbors, non-governmental agencies, and government departments. They share information with the security managers at places as diverse as the Red Cross and the State Department. "These are all our neighbors and we do exercises four times a year and meet four times a year to keep each other abreast of what is happening."

These neighbors are in addition to such agencies as the Washington, D.C., fire, medical, and police organizations and the U.S. Department of Homeland Security.

"This is so we understand what the public sector will do," Petrie explains. "That is empowering because we won't be a burden to them."

Constant Review

While GWU has great systems now, Petrie and others at the school are always looking for new ways to manage emergencies and communication.

That is actually how he found himself at the school. "George Washington had very good systems for the world that existed on September 10, 2001," says Petrie, whose position was created after the 9/11 attacks. "They realized there were some real challenges to communicate with the community here, so since that time we've built redundant communications, power, and connectivity, and we've set sustainability criteria for our contractors."

Petrie, who was part of the Navy for 35 years and had a subspecialty in operational communications, was able to spend time at New York University after the tragedies to learn how the school was affected.

He and other IT planners at GWU, whom he calls "the most incredible and talented people," have a recipe for success to share in the university community as well as in other industries and enterprises dealing with preparedness. Like a good pasta chef, they know what's cooking.

Curt Harler is a freelance writer and contributing editor for the ACUTA Journal. He can be reached at curt@curtharler.com.

Jennifer Paire is a freelance writer based in Canton, Georgia, who covers security-related topics. She can be reached at jenniferpaire@alltel.net.
In the Face of Disaster

Thinking about all the terrible things that can go wrong with our carefully designed and maintained systems and processes could drive us crazy. Fires, earthquakes, hurricanes, floods, and tornadoes—and that's just what we get from Mother Nature. Ask Pepperdine University in California about natural disasters. They know what it feels like to be threatened by fire. Disasters at Virginia Tech and the University of Kentucky were the direct results of human action or inaction, which can have a different but equally devastating impact. Although there is a vast array of events that could devastate and destroy, they share common threads when they intersect with the lives of people and the systems people create.

Saving lives, reducing losses, and maintaining service throughout these unfortunate events are the driving forces behind emergency and disaster planning efforts. Recovery after the event must be swift and comprehensive. Where do we begin, and what do we do to prepare for the unpredictable actions of natural forces and human behavior?

Four Basic Steps

In general, emergency preparedness professionals recommend the following four steps in any plan, whether for an individual or an organization:

1. Protect our ability to survive and to meet basic needs.
   Just as we should think about what our family might need if we must quickly evacuate our home, university evacuation routes and plans must also be in place and tested and practiced. Quick response is critical. When the Malibu Canyon wildfire reached the campus of Pepperdine University, many became aware of the imminent danger only when the lights went out.

2. Protect your ability to communicate and sustain communications.
   When emergencies happen, your first thought is the welfare of your family, and communication becomes the priority. The same is true in any organization facing a disaster, natural or manmade. The success of any emergency/disaster plan hinges on sustained and dependable communications.

3. Protect your important information and your ability to retrieve it.
   No amount of planning will guarantee you can save everything. The startling swiftness of the fire which consumed the contents of the administration building at the University of Kentucky in 2001 demonstrates the potential totality of the loss in a fire. (See cover photo.) If you cannot replace it, protect it or back it up.

4. Protect and develop relationships with community agencies and resources.
   Tragedies such as the shootings at Virginia Tech point up the critical need to open and maintain communications with local law enforcement and government agencies. The complex web of laws that protect individual privacy seem almost at war with the technological tools available to mine the data and sift through it all,
if only to give some indication of the danger lurking in our midst. A vast army of emergency experts live nearby: Police, fire, and civil authorities prepare communities for action in disaster situations. We should not tackle the problem alone.

**Example: Pepperdine University and the Malibu Canyon Fire**

In October 2007, the Southern California wildfires burned a half-million acres, threatening Pepperdine University’s campus at Malibu, requiring quick action by officials to ensure the safety of students, faculty, and staff on campus or in surrounding areas.

There is little doubt of the terrible cost of the California wildfires for the residents of a state sometimes referred to as a theme park for natural disasters. Fires destroyed residences, including those of university faculty, in the surrounding hills. All major roads leading into (and out of) the campus were closed by smoke and fire. Buildings on the edges of campus were damaged, with the fire approaching within 100 feet of university buildings, including the data center.

In a recent 3n (National Notification Network: http://www.3nonline.com) webinar, “The Southern California Wildfires and Pepperdine University’s Emergency Response,” Phil E. Phillips, chief administrative officer of Pepperdine University, outlined the university’s three keys to emergency preparation:

1. Develop practical and specific plans. There is no way to prevent all loss in all circumstances.
2. Forge agency relationships with fire and police entities.
3. Appoint appropriate people, systems, and procedures to address conceivable scenarios.

Phillips said that with many students, faculty, and staff living on campus or in surrounding areas threatened by the fires, university officials acted quickly to ensure the campus community’s safety, crediting the means used to alert the campus. These included a system put in just before the fires by 3n. This system uses voice and text messaging, instant messaging, pages, and other tools to keep people informed in a disaster. The same system was installed at Virginia Tech after the April 2007 shootings.

The dependable communications and the established relationships with the firefighters battling the blaze on the fringes of their campus permitted staff to remain in the data center operations area as long as the building fire- and smoke-detection system was not triggered by outside smoke...
or fire. Five notifications were sent out during the first day, including two messages providing instructions for faculty and students to move from their classrooms and dorm residences to campus safety areas.

In an October 22, 2007, Computerworld article, Timothy Chester, CIO at Pepperdine, said that because wildfires are an ongoing threat in the area, the university is prepared for that threat and others. It routinely sends its backup tapes to Iron Mountain, Inc., for protection. He said that on the day of the disaster—within 35 minutes—the latest tape backup copies were moved to a fireproof safe, the ERP applications were shut down, and the hard drives were removed and safely stored.

Mark Ladin, a vice president at 3n, said the command challenges to mass communication in a crisis or disaster include: delivering localized messages that reach their targets, notifying employees and colleagues quickly, reaching people on virtually any device, conducting immediate briefings with security and response teams, reducing miscommunication, sending consistent messages, improving effectiveness by eliminating single points of failure, and using two-way communications to ensure that everyone gets the message.

Rules of thumb for selecting effective emergency communication systems include the following:

1. Ease of use: Complex systems and emergencies are incompatible.
2. Ability to access all communications paths: This includes voice, e-mail, native SMS text messaging, instant messaging, and more.
3. Third-generation infrastructure: Constant availability, universal access, and quick response are vital elements.
4. Ease of integration: The system should integrate easily with existing systems and be scalable.

5. Rapid deployment: Emergencies and disasters won’t wait until an organization is ready.
6. An experienced provider: Someone familiar with serving the unique needs of higher education will provide better service.

Reassessing the 72-hour Rule
It doesn’t take a hurricane or flood to cause severe water damage. On May 15, 2001, fire destroyed the second and third floors of the Administration Building on the University of Kentucky campus. However, the lower floors also received extensive damage from water used to fight the fire. The rebuilt Administration Building reopened October 25, 2004, at a cost of $17,350,000 with more floor space and new facilities. No amount of money, however, could replace lost data that was not backed up and stored off-site.

An old standard in disaster planning and disaster recovery is called the 72-hour rule. It states that a facility should be cut off from access for no more than 72 hours and should be prepared to survive that long until assistance arrives. Disasters such as the 9/11 terrorist attacks, the fire at the University of Kentucky, Hurricane Katrina, and the California wildfires demonstrate the fallacy of this upper limit. Some disasters are simply so sweeping and so swift as to trim that time-limit to seconds. The only way to recover from such disasters is through advance planning and consideration of all possible scenarios, from floods to fire, from hackers to hurricanes, and from tornadoes to terrorism.

If we manage to achieve survival goals and stay in communication, the next step is data salvage, recovery, and/or reconstruction. Simply running backup tapes and keeping them in a “safe” place may not be enough. Fires can cook data disks and tape to data dust. Attempts at data recovery after Hurricane Katrina illustrated the hidden dangers from flood waters. Even storage disks that survived the water suffered from both the toxins in the brackish flood waters and the dangerous molds that grow in their aftermath. Options for off-site storage abound, but we must consider how far away is far enough.

When Hurricane Katrina struck, landlines were cut and cell phone communications were eliminated when the towers became inoperative. Lack of communications was a critical problem. One system that continued working was satellite communications, leading to the conclusion that a few satellite phones and/or a terminal for low-rate data could help in the event of a much more extensive disaster.

Off-site storage solutions are becoming common, but not common enough. Iron Mountain (http://www.ironmountain.com), a storage solution provider favored by Pepperdine, UC Berkeley, and other California educational institutions, asks on their website: “Did you know that 65 percent of public and private organizations do not have an enterprise-wide records management policy and program?” It boggles the mind to consider all the valuable data stored on individual workstations...
and notebook computers on any given campus, often without any regular data backup or security considerations other than the common sense efforts of the user. As Iron Mountain says, “Hope is not a plan for disaster.”

Navigating in the Wake
These natural disasters and human tragedies have tested the emergency systems at colleges and universities that thought themselves prepared. Some, like Virginia Tech and University of Kentucky, learned some difficult and costly lessons. Others, like Pepperdine University, were tested and met the challenge, but learned how fragile even the most advanced systems can be. All three educational institutions have moved past the disasters and developed new and more extensive emergency plans, which focus on communication with all concerned—students, faculty, staff, officers, and the community. To read more about their efforts, check out their emergency planning websites: http://emergency.pepperdine.edu; http://ehs.uky.edu; and http://www.ehss.vt.edu/Programs/OSD/Emergency%20Planning/01_introduction.htm.

It is clear that the scope of potential tragedies could drive us crazy, but it is encouraging to see colleges and universities responding to the broadest possible set of threats with creative thought, consistent training, and cutting-edge technology.

Elwin “Mick” McKellar is a freelance writer and frequent contributor to the ACUTA Journal who lives in Michigan. Reach him at mick@pasty.net.
Recent tragedies on college campuses have directed attention toward emergency notification systems, but the need for such systems is not new. Elementary schools have long practiced fire drills, sounding alarms in every classroom. Cities require homeowners to install and test smoke alarms. And most American schoolchildren learn of Paul Revere's midnight ride and how a code was developed using lanterns—one if by land, two if by sea—to signal the British advance. All these examples, old and new, hammer home the same message: An emergency notification plan is an essential and admirable precaution.

Today, a number of regulatory, societal, and technological events have made emergency notification systems more important and potentially more effective than ever. The Clery Act, so named by Congress in 1998 to memorialize a student murder victim, mandates that colleges “issue timely warnings of crimes.” Watchdog groups such as Security on Campus, Inc., lobby for safer campus environments and the disclosure of dangers. And instant communication devices surround us at home and on the go, allowing emergency notification systems to play an important role in saving lives.

In response, many communications professionals at college and university campuses are implementing emergency notification systems. The good news is that the technology landscape in the United States allows colleges to leverage the widespread use of cell phones, text messages, and e-mail to develop effective, low-cost systems that can be put to a variety of uses, not just during an emergency. Notifications fall into two broad categories that we call everyday notifications and “someday” notifications.

**Everyday and Someday**

Many university administrators face the dilemma of how to afford an emergency notification system they may need to use someday, while also managing operations everyday. To cope with an emergency that may happen someday—whether a hurricane or other natural disaster, accident, or criminal act—administrators need notification systems that can immediately broadcast alerts over a variety of communication devices to large populations. Ideally, emergency systems should also be equipped with interactive response technologies that allow recipients to acknowledge messages, so administrators can be sure everyone was reached.

But while preparation for emergency use is crucial, colleges also need an everyday system to communicate with students, faculty, and staff about routine matters: class registration deadlines, orientation sessions, financial aid and scholarship opportunities, and more. The way to afford both an everyday and a someday system is with an application that performs both functions. Such a notification system allows colleges to amortize system costs down to just pennies per day per user.
Solutions that combine the safety of off-premise hosting with Web-based easy access offer the best approach. The benefits of a hosted approach include flexible and on-demand scalability, secure availability, and reduced up-front and ongoing expenditures. Web-based systems allow anywhere access and eliminate long-distance phone charges. Together, these two assets allow you to benefit from your notification system everyday, while also remaining ready to respond to a crisis someday.

But regardless of whether your notification system is performing an everyday or a someday task, a key to its success is “pushing” information to the recipient.

Always in Touch
People have never been more accessible. More than 200 million Americans own a cell phone, a number equal to 65 percent of the country's population. For Americans of college age, cell phone ownership is an even higher 85 percent, though at times it seems nothing less than 100 percent. And voice communications over those phones are being given a run for their money by SMS text messages. In 2005, users sent 25 billion text messages, up from just 3 billion in 2004. When college students are not commun-
and distribution of both voice and text messages. A single send command will then launch these messages to the appropriate devices.

In addition, notification systems should allow administrators to choose how to send voice communications. For example, users should be able to record custom messages in their own voice, launch pre-recorded voice messages, or use text-to-speech (TTS) technology so that text messages can be converted to voice communications when that is the most convenient.

**Customized Delivery**

Segmentation is essential, because even alerts that need to be sent to the entire campus community require customization. The campus community includes students living on campus, those living off campus, professors, instructors, and maintenance employees. A notification system must be able to deliver customized messages to each group.

And most notifications will affect only certain populations, such as athletes who use the gym that is affected by a power outage, chemistry students who need to avoid a noxious spill in the lab, or freshmen who must attend orientation. Notification systems must be flexible enough to treat each scenario individually to ensure that the system remains a respected and heeded source.

"Campus administrators must guard against the 'boy-who-cried-wolf' syndrome," said Kevin Keehn, director, to receive notifications according to her personal preferences. On the most basic level, this means that students who want SMS messages will be reached that way, and those who want voice messages will receive that kind of alert. Beyond that, individuals must also be contacted in the appropriate language, and via multiple means, including anything from voice, text, or e-mail to messages on a phone machine or fax transmissions.

These notifications are too often thought of as a one-way street, but recipients should be able to respond to the alert to provide—or request—additional information.
The (Overlooked) Return Wave

There is an understandable bias built into our way of thinking about notification systems. Even the name—notification—implies that these systems are responsible only for messages going out from the center to the periphery, from the administration to the community. It is time to re-think this paradigm.

“Notification systems should provide recipients with clear instructions, including how to reply and how those who need additional details can access that information. Without a clear response path, text messages can create an avalanche of curiosity that overwhelms local government agencies,” said Keehn, Genesys. “Many college towns have small police departments that will not be able to respond to calls from tens of thousands of students alerted by campus administrators. Colleges have to handle the questions their systems generate.”

Experts at Genesys refer to the calls generated by alerts as “the return wave.” This secondary volume of calls must be anticipated, and properly designed systems must handle them as part of the notification process. For example, a notification should include options for the recipient to push 9 on a keypad for more information or * if she wishes to report important information. The system can recognize the recipient by her phone number or other address and deliver her to the proper resource, which could be a blend of self- and agent-assisted service, e-mail response, or Web chat.

“The most sophisticated emergency response systems support using the keypad or voice recognition technologies and subsequent routing of the return wave,” said Landoline, Yankee Group. “Genesys perfected its routing engine to handle massive volumes according to virtually infinite rules to ensure that incoming communications get delivered immediately to the proper resource.”

The deployment of “return wave” technologies brings the additional benefit of deeper thinking about the aims of emergency notification. With the ability to collect information from alert recipients, universities will need to develop policies about how such information is routed and over its notification system. Many students never received the messages they had signed up to receive. The incident hammered home the need for reporting and analytic tools that can reveal system performance.

“Reporting is crucial to track system performance,” said Rutledge, Genesys. “Colleges must be able to document the reliability of their systems to demonstrate performance, fix failures, and support spending requests.”

After-the-fact reporting is not enough. Real-time reporting is essential to ensure that everyone is reached in a timely fashion. Administrators should demand solutions offering real-time metrics so that problems can be identified and corrected as soon as they occur.

Conclusion

Anyone who enters the realm of emergency notification also enters the world of traditional wisdom. Proverbs have long warned us to be careful. Carpenters say, “Measure twice, cut once.” Parents say, “Look before you leap.” A Chinese proverb advises, “Don’t test the depth of the water with both feet.”

To this we would add, “Before buying, request a demo.” The best notification system is one that does what it promises and is backed up by a company that believes in its product, its reputation, and its customers.

To request a demo, please call Bill Grabner, director, government and higher education solutions, at 916/409-0952. To learn why Computer Interaction Solutions named the Genesys Emergency Preparedness solution one of the 2007 products of the year, please visit www.genesyslab.com/notification/university.
University Approaches to Emergencies and Emergency Communication

Ron Kovac, Ph.D.
Ball State University

In the summer of 2007, in response to tragic events on the Virginia Tech campus, ACUTA conducted a webinar on emergency notification response plans. The webinar garnered one of the highest participation rates ever for an ACUTA online event, indicating the high level of interest and sense of urgency that colleges and universities now had for their ability to respond to emergencies, including notification of everyone who might be affected.

After this webinar, ACUTA asked member institutions to submit copies of their emergency response plans so we could compile them and present some useful observations. Our goal was to summarize the key points, essentially creating a “table of contents” that institutions can fill in based on their unique situations and needs. What follows is what we learned from campuses that responded by sending us their plans.

From institutions of all sizes we received plans that ranged in size from two to more than 100 pages. Some covered emergency response plans for the entire university, some just for the IT department. None of the plans was considered a final version; each one was in some stage of planning or revision.

The plans were all sent to ACUTA electronically and typically existed on paper back at the home institutions. Many sites noted that their plan was also on a website so that it could be accessed from afar and by many people. The main goal was to store the plan away from where the emergency would take place.

As we reviewed and analyzed each plan, the commonalities surfaced. At the most basic level, each plan had three major sections: (1) the preliminaries, which provide justification, intent, and other background information; (2) the body, which provides the response scheme to emergencies; and (3) supporting material.

1. The Preliminaries

The first section, the preliminaries, laid down the directions and foundation for the remainder of the plan. It was here that the complex issues, strategies, and philosophies of the creators were formed. The major elements in this section included the following:

• Purpose and scope. Almost all plans started with a description of the plan’s purpose, scope, and justification. Was this plan for the entire university, the IT department, satellite campuses, or a combination?

Often the strategy taken was whom to contact and what to fix rather than how to specifically respond to predetermined events. Always, the plan was cited as a place to get information quickly that is accurate and up-to-date. Knowing that emergencies call for creative thinking and quick decisions, the plan was often thought of as a place to find information so that on-the-fly decisions could be made quickly.

• Declaration of emergency. This part discussed who can declare an emergency. This was often the university president, or a delegate so named, in counsel with campus police and university counsel.

• Goals of the plan. Clearly defined goals came next. Often the first ones were saving lives and controlling the emergency. Sustainability of university resources was often a goal through a delineation of business continuity plans. A typical goal read “Emergencies or potential emergencies be handled in a professional, orderly, and quick manner to minimize negative effects and optimize restoration.”
Confidentiality of information. Realizing the legal specter institutions face, the plan usually discussed what type of information can be released. Realizing that names and specifics should not and cannot be given to the media until other events transpired, rules of engagement with the media and the public were laid out.

Media talking points. Commensurate with the former subsection, talking points for media relations were frequently included. Often a media staging area was identified, and personnel were named who were authorized to talk with the media.

Team formation and composition. This subsection created the emergency response team and noted its composition by title and name. Team authority, role, and chain of command were clearly laid out. Typical members of this committee included representatives from the insurance company, university communications, legal counsel, human resources, public safety, and hazmat.

Emergency framework. Different universities broke down emergencies in different ways. But they all tended to have various criteria for categorizing emergencies. Common criteria included the following:

a. Scope. These criteria rated the emergency for its scope of reach. For example: community, full university, section of university, building.

b. Type. These criteria defined the type of emergency. Categories typically used in emergency type were environmental, facility, and human.

c. Intention. In this rating the intention behind the emergency was rated. The two categories used were intentional (i.e., a bombing) and unintentional (i.e., a tornado).

Often emergency plans detailed some of the crises that might arise.

The following are examples:

- Health
- Fire
- Missing child/abduction
- Quarantine
- Death or severe injury
- Natural disaster
- Tornado
- Biological threat
- Hostage situation
- Structural failure

Chemical or radiation spill
Loss of potable water or water pressure
Psychological crisis
Violent activity
Downed aircraft
Earthquake
Threat to public welfare
Bomb threat
Physical plant failure
Fleet vehicle accident/breakdown

Testing of plan. Almost all plans defined how frequently to test the plan. Often ranging from every three months to yearly, the team would meet and go through all the motions of responding to an actual emergency.

Are you aware... of the 911 barrier that your PBX, MLTS, or VoIP system creates?

Emergency responders may not be able to locate you when you need it most without precise location information. Visit www.911ETC.com and see why hundreds of Enterprises, Universities, State / Local Governments and Healthcare Institutions have turned to 911 ETC, Inc. for the automated, affordable solution.

www.911ETC.com

Precise, Enhanced 911 Location Information

1604 Hewitt Ave., Suite 401, Everett, WA 98201 / Phone: (425) 368-2911
1300 Pennsylvania Ave., N.W Suite 700, Washington, D.C. 20004 / Phone: (202) 306-9313
2. Body of the Plan

After the preliminary section (the why and what), with roles and definitions articulated, the plans attempted to describe the how. The body of the plan, the bulk of the plan, described the response to various incidents. The following were common to most strategies:

• Implementation plan. The plans took one of two approaches. Some described the response by incident type (i.e., if a tornado strikes, follow these steps). Some plans were very detailed, noting every specific step to be done by incident type. Others were more general and provided available response patterns that could be selected by the emergency response team.

• Time line. Articulated defined were the “must dos” in the first hour, first 12 hours, first day, first 3 days, and finally post-mortem. Often these steps involved notification of parties within and outside the university.

• Business continuity plan. Some plans included separate steps for maintaining crucial institutional services such as dormitory meals, heating, phone service, electricity, computer systems and applications, and records.

• Assembly areas. Most plans defined where students and staff should assemble for evacuation, control, or safety. In some cases, this was an off-campus site.

3. Supporting Materials

• Contact information. All plans included key contact information for members of the emergency response team and all other pertinent staff in the university and community. Information included cell number, home phone, e-mail, land mail address, and so on. In addition, an external contact list was often provided. On this list were key vendors who could help in attenuating the emergency.

• Calling tree. Some of the plans incorporated a calling tree to make use of the personnel to spread the word quickly. In this case, the tree and all contact information were provided.

• Utility system descriptions. Description, layouts, and drawings of all utility systems were provided. This included telephone, electricity, gas, and data.

• Building floor plans. Floor plans for each building were either incorporated into the plan or available on a CD. These were considered essential for rescue, evacuation, or public safety issues.

• Annual review process. A process was often defined to update the plan at least annually. At the simplest, this was to account for changes in personnel and phone numbers, moving, and building adaptation. At the most complex, it was to plan for emergencies that are new to university locations.

• Temporary morgue location. Recognizing that deaths may result from emergencies, some of the plans allowed for a temporary morgue. For colleges in small towns with limited public resources, this was thought to be essential.

• Notification resources available and how to access. Often the plans noted all the available ways to notify students, parents, staff, faculty, and others. Contact and password information was provided for each of these so the full emergency response team could implement the plan response. The notification resources were broken down into categories: active and passive broadcasts.

Active broadcasts included such things as sirens and public address systems.

Passive broadcasts included some traditional methods as well as some newer technologies:

AM and FM stations  
E-mail blasts  
Fax blasts  
Message injection/video systems  
Web page notification  
Messaging  
Instant messaging  
Television stations  
Pager blasts  
Cellular blasts  
MOTD  
FX Lines  
Cell phone  
Other

• Prior arrangements. This section discussed prior arrangements made with vendors or others for a alternate functional spaces as well as a command center. Examples are arrangements with telcos and IXCs, major vendors, and emergency service providers.

Summary

We realize that no single plan or solution can work for all institutions. However, we believe that certain common elements can be incorporated into all such plans, and certain technologies are an important part of any emergency response plan.

Possibly the plan is not the end at all, but rather the planning process is. In the words of the immortal leader Dwight Eisenhower, “In preparing for battle, I have always found that plans are useless, but planning is indispensable.”

IT professionals are used to planning for disasters in order to maintain the mission-critical nature of their systems. This is in our blood. This skill set can be used to assist in the development, adaptation, updating, and implementation of the emergency response plan for an institution.

Ron Kovac, PhD, is director of training and professor of information and communications sciences at Ball State University. He can be reached at rkovac@bsu.edu.
A Reasoned Response to Crisis

Crisis management teams expect to encounter evidence of massive material loss at the site of a disaster. However, when the Firestorm Solutions team received a call from Charles Steger, Virginia Tech’s president, to provide on-site crisis management support following the tragic campus shootings in April 2007, what they saw was little more than the ribbon of police tape around stolid Norris Hall and a horde of media satellite trucks.

The immediate as well as long-term result of the Virginia Tech tragedy has been dramatically heightened concerns about campus security coast to coast. Initial responses based on everything from emergency messaging and alert systems to self-defense training programs are being sold to campuses around the country.

Certainly, each added layer of preparedness is an improvement. Still, the VT shooter managed to circumvent a number of protective measures, including dorm security locks, and law enforcement officials agree that a suicide assassin—one who intends to kill as many people as possible and die in the process—is almost impossible to stop.

Because every crisis is a human crisis, we must look for ways to mitigate the damage. There is no single panacea; the reasoned response requires a shift in policies, procedures, and attitudes. Equipment, hardware, and software alone can’t protect people. There must be a new environment of personal knowledge and responsibility.

**Predict. Plan. Perform.**

Continuity planning is a strategic governance issue. Proper disaster planning requires that you *predict* the vulnerability, *plan* the response, and *perform* when the event occurs. A well-designed and -executed plan can transform a crisis. Features of a well-designed plan include an analysis of all vulnerabilities and their impacts on the people, processes, and assets. A well-defined plan will identify how these impacts can be mitigated in a crisis. And a well-defined plan will have detailed training, testing, and updating features. The goal of every plan should be to mitigate the impact and accelerate the return of normal operations.

People are trained to react; we need to learn to pre-act. Pre-action is a noun that means (1) the act or process of preparing prior to a crisis, disaster, treatment, situation, or stimulus or (2) the detailed development, implementation, and testing of a plan in advance of need. Time restricts the quantity and quality of options that we have in any crisis or disaster situation. The less notice we have, the fewer options and the greater the impacts of a disaster or crisis. Today, most vulnerabilities and exposures are foreseeable to the trained eye. Predicting the threats and risks we potentially face requires an analysis of the site, processes, people, materials, and information within an organization.

Once vulnerabilities have been identified, planning can be done to mitigate these exposures and determine optimal recovery strategies in light of operational, strategic, and external issues. No plan is going to solve or prevent every crisis, but it can minimize many of the undesirable outcomes.

Finally, in order for people to perform when needed, plans must be communi-
cated, tested, and updated on a regular basis, and everyone should be involved. Changing the mind-set of “disaster denial” means accepting the possibility of a crisis and expecting everyone to be as prepared as possible.

Fostering awareness leads to a culture of preparedness. Most incidences of violence in schools, be it intruder, student-on-student targeted violence, or even terrorism, could have been prevented if someone had acted on what they knew.

Lessons Learned
1. Vulnerabilities exist. Despite the disaster denial mind-set of many in our society, the fact remains that vulnerabilities are everywhere. Could any university president deny that what happened at Virginia Tech could have happened at his or her school? What about the increasing threat of natural disasters, acts of terrorism, or the looming likelihood of an avian flu pandemic? What about security issues and campus safety, including identifying and reporting suspicious persons, sexual harassment, and mental health challenges? It can be a challenge to walk the line between fear and denial, but acknowledging these realities is the first step in mitigating them.

2. Planning is critical. People—not just hardware or software—will make the decisions that save or cost lives. Who will press the button to send out the warning message? What if he or she isn’t present when it needs to be done? Are prewritten messages authorized and readily available? What specific developments will trigger what response? What will be the chain of command? What are the roles and responsibilities of all those involved? What is the process for students to evacuate dorms, classrooms, and the campus? How will students, faculty, and staff report their safety and be accounted for? These are decisions that need to be made and communicated in advance.

3. Training and testing are not optional. In an environment such as a college campus—with the average 30 percent turnover in student population—training needs to be repetitive and specific. If people don’t know their roles in the plan, there really isn’t one. The training, in addition to making faculty and staff aware of their duties under the plan, should increase everyone’s awareness of preparedness issues. Testing demonstrates areas where plans require modification. Review, testing, and training will ensure long-term viability.

4. Prepare to communicate. By delivering key messages to the community in a timely fashion, the consequences of a disaster can be managed. Because of good communications at Virginia Tech, freshman enrollment projections for the fall semester were met. Confidence in the university’s leadership was renewed, as initial calls for resignations were replaced by overwhelming statements of support.

5. Anyone may be held accountable. While the liabilities involved in the Virginia Tech event are uncertain, higher education in general has been put on notice. It should no longer be assumed that certain kinds of events can be called “unforeseen.”

A Call to Action

Over the coming months and years all university constituents—parents, faculty, staff, alumni, and media—will want to know what was learned and what improvements have been made since the events on Virginia Tech’s campus. Immediately, we saw an increased awareness of security weaknesses and the beginning of a culture of preparedness on most campuses. A simple solution to this complex problem doesn’t exist, but the importance of planning has come home to us all.

James W. Satterfield is president and chief operating officer of Firestorm Solutions, a strategic consulting firm that focuses on vulnerability analysis, threat assessment, and exposure mitigation. Visit Firestorm at www.firestorm.com.
Digital Forensics: What Is It and Why Should I Care?

Ron Kovac, Ph.D.
Ball State University

Although the word *forensics* is not new, we hear it a lot more often these days. Certainly TV crime shows, such as *CSI* and *Law and Order*, have put a spotlight on the science and art of forensics, especially digital forensics.

Digital forensics may be broadly defined as finding and obtaining information residing on digital devices and then creating a detailed analysis of it. *Digital devices* means any digital device: laptop or desktop computers, thumb drives, PDAs, cell phones, or even GPS devices. The ultimate aim of this process is to use the information as evidence in policy violations or civil or criminal court cases.

Almost all digital devices store information in either volatile or nonvolatile memory, and information can be pivotal in acquiring and processing evidence in an investigation. Even data thought to have been erased can often be retrieved to provide evidence in a case.

But the field of digital forensics is more complicated than that. Often the discipline of digital forensics is broken down into three major areas: computer forensics, network forensics, and vulnerability assessment and risk management.

In the computer forensics area, formal forensic analysis of systems (most often hard drives) is accomplished looking for evidence related to an incident or crime.

In the network forensics area, analysis is done on how perpetrators use the network to further the crime (e-mail, file transfer), and where they went and what they did on the network. Remember, the network is the roadway system between computers, and all network equipment can log every packet.

The last area, vulnerability assessment and risk management, tests the integrity of digital devices around the campus or enterprise. This aspect of computer forensics focuses on preventing hacking into current systems and stealing or corrupting data.

**Why Should I Care?**

There are certainly enough issues to keep IT professionals in colleges and universities busy: infrastructure, strategic planning, new technologies, funding, and more. But when computer crime appears likely, our attention turns to political and law enforcement measures. It is better to be prepared for these possibilities with some knowledge and a game plan. The following actual scenarios have occurred recently on college campuses:

1. The president’s office calls to complain of hostile and threatening e-mail coming to her office from within the campus. Who is doing this?
2. The Secret Service calls charging that e-mail threatening the president of the United States is emanating from your campus. Find the culprit and get evidence.
3. A rogue faculty member is suspected of running a business from his office. A bullet-proof case must be developed.
4. Computer facilities on your campus are being used as zombies in attacks against large corporations. A lawsuit has been filed against the university.
5. Downloading and distribution of large amounts of video and music files are coming from your campus. The RIAA has filed a lawsuit.
All of these events require immediate action on the part of IT professionals who may—or may not—be familiar with digital forensics.

**Digital Forensics Investigations**

Soon after the attacks on the World Trade Center in 2001, thousands of people were involved in an intensive forensic analysis of the cause, damage, deaths, and probable suspects in this tragic event. The results were startling, and law enforcement personnel were able to piece together a jigsaw puzzle of amazing proportions. But the forensic analysis did not involve just physical evidence; it involved digital forensic evidence where the FBI attempted to, and did, find evidence on digital media and transmissions to ultimately identify and bring some of the perpetrators to trial.

Colleges and their information technology infrastructures are porous entities meant to provide convenience to the user, often at the sacrifice of security and accountability. But this does not negate the need to maintain accountability and stop the promotion of terrorism, threats, policy violations, and money laundering from within campuses. Digital forensics provides the ability to track users suspected of violating campus policies and to assist outside law enforcement agencies in identifying criminal activity.

The role of the IT professionals, and especially forensics experts, is to collect and analyze evidence from digital devices to determine whether a crime has been committed or policy violated. If, after this step, the evidence is inculpatory (pointing to a legal or policy violation) and not exculpatory (clearing the suspect of wrongdoing) a case needs to be prepared—artifacts, evidence, and opinions that will be offered in court or at a company inquiry. Before beginning the investigation, a plan must be followed and accepted procedure must be used to prepare the case. Approaching the case haphazardly will usually destroy evidence or make the evidence not legally admissible.

In order for a case to be made, a plan and systematic approach must be developed. This process takes time, and cannot be rushed if the intent is a case that will hold up in court. Such a plan will usually include the following six steps:

1. Develop an initial theory and assessment about the case. During this stage a firm understanding of the situation being investigated must be developed. All specifics of the case must be known: the type of evidence that can be used (PDA, hard disk), the operating system used, disk format, intention of the perpetrator, and location of the evidence.

2. Obtain the evidence and make perfect copies. After securing the evidence, perfect-image copies or bit-stream copies, in multiple, must be made. A bit-stream copy is a bit-by-bit copy of the original storage medium and is an exact duplicate of the original disk—vastly different from a simple backup copy of a disk. In addition, a chain of custody for the evidence trail must be maintained noting where the evidence has been, who has handled it, how it was secured, and so on, in order to maintain legally admissible evidence for court or in a company trial.

3. Develop a detailed design, determine resources, and test the design. This stage involves preparing general and detailed steps to be followed. The detailed design estimates the amount of time needed and helps the process stay on track while also delineating the forensic workstation requirements and the other tools needed. During this step, the design should also be tested by comparing hash signatures to ensure that proper copies were made. Hashing is the process of using a unique mathematical algorithm to snapshot the current state of a file, substance, letter, etc., so that it can be noted if any changes occurred to the document during storage, transmission, or processing.

4. Identify and mitigate the risks. During this stage an understanding of the incident must be made to assess risk and whether a crime occurred or policy has been violated. Usually to mitigate risks, multiple copies of the original evidence are made so that destruction of a single copy does not endanger the case.

5. Analyze and investigate the data held as evidence. In this stage, the forensic workstation, software, and hardware tools are used to analyze the copies of the evidence. This is a complex undertaking, as viewing the data can sometimes alter it. For example, Microsoft Windows can sometimes alter the files on the disk and the integrity of the evidence, making it useless in a court case. Write-blocking software can be used to prevent Windows from altering the integrity of the evidence. The task is to recover data that can be used as evidence. This involves going through file fragments and deleted files. The goal is to find the evidence (pornographic files, evidence of emails sent and received, timestamps of use, etc.) to determine if a crime has been committed or policy violated.

6. Develop the case report. During this stage, a case report is written giving a historical account of all the steps taken and all the evidence found. Who, what, when, where, and why are basic facts that must be provided.

**Proceding with an Investigation**

If an incident, like any of the scenarios outlined occurs, what do you do? Law enforcement entities have different rules by which to abide that are more stringent, while private-sector organizations (business and government agencies that are not involved in law enforcement) have more latitude. In the United States, private-sec-
tor agencies must comply with state public disclosure and federal Freedom of Information Act law and make the documents they find available as public records.

Investigations of computer incidents often happen in a controlled workplace, rather than a home, and involve a policy violation rather than a crime. Most often the equipment used to violate the policy is owned by the organization and therefore known to the organization and is running "standard" operating system, e-mail, and Web browser facilities. This makes the job of the digital forensics expert far easier.

What is seized and analyzed from an employee depends on published college or university policy. The Fourth Amendment of the Constitution provides American citizens the expectation of privacy. A well-defined university policy provides the employer the right to examine, inspect, or access any company-owned computer equipment. If this policy is created and disseminated, an employer can legally access all computing assets without Fourth Amendment privacy rights being violated. Warning banners on the log-in screen are often used to alert employees of policy statements. This provides the employer the right to freely initiate inquiries to determine if an infraction has occurred. This is a tremendous advantage over law enforcement agencies (public entities), which require a warrant, with the prerequisite probable cause.

Even with policy and warning banners in place, an organization should not delve into employees' computers without some reasonable suspicion. A well-defined process that describes the initiation of an investigation should be put into place, and the process must be followed before an employee's privacy is violated.

A journal or, preferably, a video recording of the acquisition should be done from the time of arrival on the scene. Time and date of arrival need to be noted, and every significant task performed documented.

Sometimes the lines of the investigation get blurred. If, during the course of a policy or abuse investigation, criminal acts are discovered, then the employer must turn over
an external device, each screen should be seized and brought back to the lab for processing. Before removing the computer, record how the wires are hooked up with close-up shots of the back of the computer. Areas around the computer should also be scanned and recorded for portable thumb drives and other pieces of evidence.

If it is not possible to remove the digital device, then a bit-stream copy of the storage mechanism must be obtained on site. If the computer is powered off, leave it off and return it to the lab for processing. If it is powered on, then a judgment call needs to be made. Standard practice is to pull the plug to halt the machine. Because so many crimes are network related, this strategy may cause damage. If powered on, it is suggested that the investigator record each screen that is on the computer, record the data that is on the screen (or save to an external hard drive), and then perform an orderly shutdown. The goal is to preserve as much evidence as possible. This goal requires a lot of judgment calls and understanding of computer and network operation. In this case, the evidence must be turned over to the proper law enforcement agencies for further action.

Public law enforcement agencies fall under far more stringent rules and need probable cause, as defined by a warrant issued by a judge. Warrants are very specific, with limiting phrases to guide law enforcement personnel to what they can look for.

Often investigations in colleges and universities do not involve seizing evidence but involve covert surveillance of employees suspected of violating stated policies. The use of covert surveillance should be clearly defined in policy and aligned with appropriate government policies.

**Table 1: Product comparison**

<table>
<thead>
<tr>
<th>Product</th>
<th>Manufacturer</th>
<th>Approximate Cost</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>EnCase</td>
<td>Guidance Software</td>
<td>$250</td>
<td>Intuitive GUI feel, Multiple platform analysis, EnScript automation module, Evidence transfer capability, Easy report writing</td>
</tr>
<tr>
<td>DriveSpy</td>
<td>Digital Intelligence</td>
<td>$200</td>
<td>Analysis of large drives, Hex viewer, Logging capabilities, Duplicate creation, Generate Md5 hash of an entire drive, Save and restore compressed images</td>
</tr>
<tr>
<td>AccessData</td>
<td>Forensic Toolkit 2.0</td>
<td>$300</td>
<td>Password recovery, Powerful search capability, Easy export, GUI interface, Data carving engine</td>
</tr>
</tbody>
</table>

Regardless of their physical structure, forensic tools do a multitude of tasks:

- The first task is to acquire and copy the original disk to ensure it does not become corrupt evidence.
- The second task is to validate the copied data to ensure it is accurate and then to discriminate the data. Discrimination involves sorting and searching through all the data to find the proverbial needle in the haystack.
- The third task of a forensic tool is to extract the required information from the raw data. This takes good search capabilities and the ability to view the data in its primal form (i.e., to view .ppt files through Microsoft PowerPoint).
- The final task of a forensic tool is reporting. This subsystem helps the investigator prepare the written report and assists in extracting data drawn directly from the evidence. Not all forensic tools have each of these features, and each of these features can have many subparts.

In Figure 1, three popular products are compared. These three products are fairly powerful, easy to use, and readily accessible.

**What Makes a Forensic Expert?**

A wide range of skills is necessary to be able to secure evidence and win a policy violation or a court case. First and foremost, experts in this field need a deep knowledge of the criminal justice system in order to capture and preserve evidence that the courts will uphold.

Second, digital forensics experts need in-depth knowledge of all the digital devices that are currently used and have been used in the past. They must understand how to capture data from the latest PDA as well as a 10-year-old Macintosh.
Third, they must understand the strict rules of investigation and evidence gathering.

One of the key associations in the digital forensics field is the International Association of Computer Investigative Specialists (IACIS). IACIS restricts membership to sworn law enforcement personnel or government employees working forensics cases. The highest level of certification is the Certified Forensic Computer Examiner (CFCE). Applicants are tested in the following areas:

1. Analyzing information on various types of disks (floppy disk, CD, and hard disk). Information on the disks is hidden, erased, or not easily assembled.
2. Creating concise and legal reports for the disks that contain the following:
   1. Exhibits of evidence
   2. Detailed lists of evidence on the disks
   3. Explanations of data/information on the disks
   4. Explanation of the procedures used

   - Data acquisition
     1. Creating a bit-stream image of a suspect disk
     2. Verifying the bit-stream image through various algorithms

   - Researching
     1. Finding owners of websites
     2. Finding support evidence on the Web

Summary

The field of digital forensics is complex and growing. IT professionals, especially in universities and colleges, must be aware of the basics of this field to do their job effectively. Certainly, situations will arise that delve into this field. It is far better to be prepared now than to face a devastating lawsuit later on.

Collegiate programs in the field of forensics, especially digital forensics, are growing by leaps and bounds. A final word of advice: It may be wise to look in your own backyard for expertise and programs that can help the IT department in this area.

Ron Kovac, Ph.D., is director of training and professor of information and communications sciences at Ball State University. He can be reached at rkovac@bsu.edu.

---

MiCTA is pleased to announce a new Emergency Notification System (ENS) contract.

**Connect-ED®**

*The NTI Group, Inc. (NTI)*

Approved

Visit our website at [www.mictatech.org](http://www.mictatech.org) for future announcements.

Save time and money by purchasing ENS through the MiCTA Program.

---

**Technology Solutions for Members Nationwide**

Offering Discounted Services Through Our Approved and Endorsed Vendors.

MiCTA, 515 N. Washington Ave., Suite 405, Saginaw, MI 48607 + micta@mictatech.org
Toll Free: (888)-964-2227 + Direct: (989)-753-2424 + Fax: (989) 753-2655 + [www.mictatech.org](http://www.mictatech.org)
Exploits, Guidelines, and Vulnerabilities: Protecting Digital Resources

According to Wikipedia, “an exploit ... is a piece of software, a chunk of data, or sequence of commands that takes advantage of a bug, glitch, or vulnerability in order to cause unintended or unanticipated behavior to occur on computer software, hardware, or something electronic (usually computerized). This frequently includes such things as gaining control of a computer system or allowing privilege escalation or a denial-of-service attack.” (http://en.wikipedia.org/wiki/Exploit_%28computer_security%29)

A recently released exploit that takes advantage of problems in Microsoft’s Routing and Remote Access Server (RRAS) has drawn the ire of Microsoft. In an advisory the company states, “Microsoft is disappointed that certain security researchers have breached the commonly accepted industry practice of withholding vulnerability data so close to update release and have published exploit code, potentially harming computer users.”

In his blog, security researcher H.D. Moore took issue with Microsoft’s comment and posted a lengthy rebuttal explaining why he chose to publish the exploit nine days after Microsoft issued its RRAS patch. Moore’s position is that there is no “commonly accepted industry practice of withholding vulnerability data so close to update release.” To argue his position he points to several companies that routinely buy unpublished exploit code and then resell the details to their customers. Such companies include VeriSign’s iDefense, Digital Armaments, and Immunity Inc.; however, these companies do not publicly publish exploit code, which seems to be the sticking point for Microsoft.1

For college and university network managers and security professionals, the notion of responsible disclosure has centered on the guidelines of the Organization for Internet Safety (OIS).2 OIS is an organization of commercial technology vendors whose role includes the development of policies and procedures relating to the public disclosure of hardware and software vulnerabilities. OIS guidelines encourage only nonpublic disclosure of hardware and software security flaws until the vendor has had an opportunity to correct them. The organization believes that vendors should be given a chance to create a fix for a vulnerability before it is made public.

The OIS guidelines have come under sharp criticism as some vulnerabilities are known months before a fix is available. The key criticism of the guidelines is that vendors have an indefinite period of time to develop a fix for a problem, leaving the product users vulnerable to security threats and potential subsequent costs, including possible litigation, damage to consumer confidence, and reduction in the value of the company itself.

More and more user organizations are arguing that they should know about vulnerabilities as soon as they are detected to minimize their exposures. Legislation such as the Health Insurance Portability and Accessiblity Act (HIPAA) and the Gramm-Leach-Bliley Act of 1999 require organizations to have a comprehensive security program to protect personal information. Although laws such as these leave much room for interpretation, the nature of these laws and the potential for subsequent litigation is elevating such decisions to prominence in terms of management decision making related to risk mitigation.3 A study by KPMG found risk management to be one of the top three challenges facing managers.4

VeriSign’s iDefense division and 3Com’s TippingPoint division have seized the opportunity to launch early-warning “security vulnerability notification service” businesses. The two companies offer an early-warning

James S. Cross, PhD
Steven A. Samaras, PhD
Longwood University

---

service for purchase by enterprises, government agencies, and software/hardware vendors. The vulnerability intelligence services deliver regular advisories and alerts with exclusive vulnerabilities discovered by their vulnerability teams as well as those public vulnerabilities that are aggregated and vetted by their staffs. The advisories help organizations identify the vulnerabilities that pose the most significant threat. Customers can learn about a vulnerability as soon as it is detected by this army of researchers. Subscribers to the service are notified at the same time that the vulnerability information is sent to the vendor whose product needs to be fixed.

Many in the industry say the OIS guidelines were a valiant effort but are now obsolete, as they were designed to help the software vendors, not the users of the vendor’s products. Some critics of OIS argue that notifying a customer of a security flaw after the vendor has a patch does nothing to minimize the customer’s risk. Many in the security community believe that OIS is nothing more than a lobbying group for the key OIS members.

The Ongoing Debate

Although OIS was formed to make it easier for the security community and vendors to work together to fix security vulnerabilities, the organization has been unable to develop a process that both sides can agree upon for discovering, disclosing, and then correcting security vulnerabilities.

A CIO/PriceWaterhouse study found that 29 percent of executives did not know how many negative security events they had experienced in the past year; 26 percent did not know what type of attacks they were and how they were accomplished; but more troubling, 50 percent of those executives did not know how much their firms were losing as a result of these attacks. The lack of any consensus related to procedures complicates as well as delays the process of fixing vulnerabilities, and ultimately increases the risk and exposure of the product users.

Despite their best efforts, organizations continue to be successfully attacked at an alarming rate. Anecdotal evidence suggests that the highly reactive perimeter-focused defensive measures employed by most organizations are simply unable to keep up with the rapidly changing threat landscape. With more threats emerging and spreading more quickly than ever before, the result is a steadily increasing degree of chaos. Ernst & Young’s Global Information Security Survey reveals that organizations are allocating more than half of their security budgets to routine operations and incident response.5

The responsible disclosure question is critical to corporate, governmental, and nonprofit boards as organizations are now confronting well-funded, organized criminal groups that quickly commoditize stolen personal, commercial, and intellectual resources for profit. In 2006, of five actions taken by the Federal Trade Commission, failure to assess risk and/or vulnerability was cited in three of those cases, and failure to monitor and defend against unauthorized access was cited for the same three.7 Because such risk is dynamic, user firms need a dynamic and sustainable risk assessment process built into ongoing fraud and security policies and procedures.

Although the OIS vendors and the security community heartily agree that software needs to be built more securely, developing a set of guidelines that both sides can agree upon has been fraught with difficulty. Such guidelines could serve to establish potential liability against one or the other side, making the guidelines even less appealing. The OIS Code of Conduct prohibits the distribution of detected product vulnerability information to anyone other than the vendors of the product. OIS contends that it is unethical to intentionally make one organization more vulnerable than another. Prerelease communities distribute the information too broadly for it to be considered a secret. Once the word is out, the risk of exploits increases dramatically, but many people outside of this community still don’t know about the problem. This potential imbalance of vulnerability information can have competitive issues as one firm in an industry can address the vulnerability through knowledge of its existence while another remains unknowingly exposed.

OIS’s position has not set well with the security community. As the security landscape continues to evolve, the:

- Threat volume is rising;
- Threat generation time is shrinking;
- Threat propagation speed is increasing;
- Threats are becoming more elusive;

Database Publishing ... problems?
We’ve got solutions!

“You don’t just do the work we pay you to do; you also help us identify and solve problems. Your friendly, conscientious and knowledgeable staff transformed our annual database publishing project from a yearly anxiety attack to a well-oiled machine.”

—Client Testimonial

DATA MANAGEMENT, INC.
5250 North Park Pl. NE, Ste. 210
Cedar Rapids, IA 52402
319/373-7773
www.dbman.com
E-mail: info@dbman.com
• Threats are becoming more sophisticated; and
• Threats are more and more focused on system/application layer weaknesses rather than network layer vulnerabilities.

Gunter Ollman, director of security at IBM’s Internet Security Systems, estimated that the 7,247 software vulnerabilities reported in 2006 represented only 5 percent of the potential number. With the number of incidents per year skyrocketing, security has become the Achilles’ heel of organizations of all sizes. Chris Sonderby, chief of the U.S. Department of Justice’s Computer Hacking and Intellectual Property Unit, states, “Some companies just don’t realize that there are dedicated hackers out there, talking to and working with other hackers, that could be trying to steal their resources. Companies need to look hard at what kind of protection they have in place.”

Protecting an organization’s digital intellectual resources involves a number of strategies, from bolstering hardware strength to informing users about proper computer usage to simple network monitoring, sophisticated techniques of data mining, and subscribing to early-warning systems/services.

Tackling Security from the Top Down
Managing security risk was rarely the focus of boardrooms at the start of the 2000 decade; but today, identifying, assessing, quantifying, and mitigating security risk is akin to a holy grail at many companies. It has become a high-level topic as corporate boards find that they may be liable if they fail to keep pace with evolving best practices. While boards were once protected by the business judgment rule, indemnification agreements, and directors and officers (D&O) insurance policies, courts are now looking beyond the traditional protections provided to directors. New legal requirements and compliance issues are mandating that corporations have a robust governance, risk, and compliance program.

Even though most regulations are directed at “for-profit” institutions, the American Bar Association warns that non-profits should also address security risks and avoid the same problems or they may be litigation targets like any other business.

Since January 2005, more than 154 million electronic data records of U.S. residents have been exposed to security breaches, according to the Privacy Rights Clearinghouse, which collects publicly reported security breaches. T.J. Maxx’s disclosure in January 2007 that it was the victim of a sophisticated hacking incident involving more than 45 million cardholder accounts underscored the magnitude of the controversy. In the T.J. Maxx case, the company indicated that it has spent more than $17 million to investigate and contain the security breach. It now faces a number of lawsuits, including a class action suit filed by the Massachusetts Bankers Association for restitution to compensate banks that had to block and reissue thousands of cardholder accounts, as well as to cover the losses due to fraud protection warranties.

Increasing consumer awareness and sensitivity to information security is increasingly requiring organizations to develop strategies to protect business value, brand reputation, integrity, and consumer loyalty. In one study, 65 percent of consumers reported that they had experienced some sort of computer security problem and more than half of those would at least strongly consider taking their business elsewhere.

The loss of consumer confidence in a trusted online community took another big hit with the discovery of a new-generation Trojan horse that encrypts files on an infected host and demands ransom payments for the decryption password.

Behind all the fury, there is still the question of whether paying big bucks for critical software/hardware hacking exploits is a good thing or is simply creating more risk. The two major players in the early warning security vulnerability notification service business contract with a cadre of independent hacker researchers from all over the world. According to Ryan Naraine, iDefense is offering $8,000 USD (plus $2000-$4,000 for a working exploit) for a remote code execution vulnerability in either IE7 or Vista. Many are outraged about the launch of the latest hacking contest that comes less than a month after researchers at Trend Micro discovered Vista flaws being hawked on underground sites for $50,000 a pop. The willingness to pay this level of money illustrates the growth of the market for information on software vulnerabilities.

TippingPoint’s manager of security, Terri Forslof, indicates that TippingPoint works with independent researchers for original information about software flaws. The more critical the information about a flaw in widely used applications, the greater the fee paid to the researcher. As to the ongoing debate about public hacking contests, Forslof states she does not agree with OIS’s and Gartners’ view about responsible disclosure and public contests because the OIS guidelines are basically dead. Although no longer relevant, she states, “The OIS standards were a valiant effort, but in the end the OIS was designed to help the vendors manage things on their end.”

To add fuel to the fire and debate, Frost & Sullivan commissioned a study...
Implications for Colleges and Universities

Some believe the demise of OIS will only make matters worse and create an unbalanced playing field. Does paying big bucks for critical software/hardware exploits make the enterprise safer? Although many in the security community are against public hacking contests, they are in favor of actively looking for vulnerabilities and notifying customers and the vendor as soon as the flaw is detected. McAfee, IBM, and others who oppose paying outside hackers for vulnerability information believe it is not safe or ethical. The critics believe it provides a bad incentive that pushes hackers “over the deep end” and creates a cottage industry of and market for unsanitized exploits.

In the midst of all this debate, the higher education community frets that the outcome for them will be substantially higher new costs for already tight budgets to subscribe to one or more of the early-warning vulnerability services. A comprehensive service can easily run over the six-digit range per year if it provides exclusive intelligence reports on topics the customer chooses as well as a dedicated analyst to support an organization security team.

Some college and university board members are also beginning to ask the tough questions about their institution’s preparedness for a cyberdisaster and what plans are in place. Others are asking what a rapid response system should entail and what is the value added of an early-warning system. Still others believe a greater awareness of developing threats means having access to proactive intelligence regarding public vulnerabilities, malicious code, geopolitical threats, and topical research papers on unfolding issues.

According to Privacy Rights Clearinghouse, a stolen laptop at the Boeing Co. pushed a widely watched tally of U.S. data breach victims past the 100 million mark in 2006. “The Boeing disclosure pushed the total number of data breach victims on the Privacy Rights Clearinghouse website to 100,152,801,” said Beth Givens, director of the consumer advocacy group. Colleges and universities were no strangers to the list in 2006. More than 30 security breaches were reported by colleges and universities from January 1, 2007, to the end of May 2007. The required reporting involved personal information useful in identity theft such as Social Security numbers, account numbers, cancelled checks, credit/debit card numbers, and driver’s license numbers.

In this chaotic security environment, what are universities to do to preserve the integrity of their reputation against very real threats, without breaking their banks? In an ideal world, what would be the best solution? How do they choose a course of action from among a list of less-than-ideal solutions to minimizing disruption, damage to institution reputation, and possible lawsuits? Tough questions don’t have easy answers.

James S. Cross, Ph.D., is dean of the College of Business and Economics at Longwood University. A past president of ACU.TA, Dr. Cross is a frequent contributor to the Journal. He can be reached at jscross@jetbroadband.com.

Steven A. Samaras, Ph.D., is an assistant professor of management at Longwood University. Reach Dr. Samaras at Samarasa@longwood.edu.

Notes


Classifying Events, Incidents, and Disasters

Determining whether an event qualifies as an actual incident or a disaster and is not just a routine event is sometimes clear, but often not. Information about the event may be incomplete at first and is sometimes contradictory, sometimes inaccurate. Should you wait and see? Investigate? Take action? And when do you notify higher managers, who will expect definitive information?

Declaration of an incident or a disaster is often thought of as a binary choice: It is or is not an incident or a disaster. But a graduated scale for classification may be more helpful, using the characteristics of the event along with the level of confidence regarding information about the situation. Classification is needed for all types of events ranging from physical (i.e., power outage, fire, or tornado) to cybersecurity (i.e., theft of personal identifying information or a system failure).

The events, once classified, need to be linked to actions such as notification, response activities, and application of resources. Thus, event classification is critical to incident and disaster response planning.

Planning Foundations: Risk Identification and Assessment

Event classification and response planning are part of risk management. An organization must inventory and prioritize its functions and assets as well as identify and assess threats and vulnerabilities. This information contributes to the development of a business impact analysis, which evaluates the potential damages from various event scenarios.

Threat agents may be natural (i.e., weather, animal or insect infestations, or disease), environmental/technological (i.e., dust particles, structural, mechanical, or software), or human. Human threats are subcategorized as deliberate (i.e., hacking, attack by a gunman), accidental (i.e., doing the wrong thing because of miscommunication or lack of training), or negligent (i.e., deliberately skipping testing before releasing a product).

Threats should not necessarily be viewed as stand-alone, as multiple threats can occur simultaneously or in close succession. Chain reactions of threats are not uncommon, either; for example, an earthquake may cut off power, which shuts down air conditioning and other systems.

Vulnerabilities are weaknesses that can simply fail or be attacked and exploited by a threat agent. Vulnerabilities may arise during design, implementation, or maintenance. This would apply to levees in New Orleans as well as to firewalls protecting your network. Vulnerabilities can also occur in policies and procedures. For example, there simply may not be a policy forbidding some specific activity—until someone finds that weakness and exploits it. Or procedures may lack a critical step or may not be followed correctly.

While identifying and prioritizing threats and vulnerabilities are important activities, current thinking from the National Institute of Standards and Technology and the Emergency Management Institute gives more weight to the impacts (or hazards) of events. In emergency management, this is termed an "all hazards" approach, looking for commonalities in events to construct action plans. Still, the scenarios that lead to the impacts need to be thoroughly understood, from various triggers that can cause an incident or disaster to the kinds of impacts that may result.

Event Characteristics

Impacts are, obviously, one key characteristic of an event, but not the only one. Other characteristics include the magnitude of the event, the event’s occurrence and onset, and perceptibility.

The most important impacts are those to safety and property. Most people think of physical threats such as a fire endangering people and property, but information and communications technologies can also create hazards. Examples would be failures of the air traffic control systems and networks or
systems that are used for critical infrastructures such as water systems, dams, and energy generation and distribution.

An event may also affect the ability of an organization to function: Its capability to perform its mission may be degraded or disrupted. In addition, there may be financial impacts, such as stolen funds or costs of response and recovery. Another potential secondary impact is legal, whether from lawsuits or regulatory fines. Finally, there is the reputation of the organization.

Consider the Federal Emergency Management Agency after Hurricane Katrina.

The magnitude of an event is closely related to its impacts. Magnitude has two dimensions: scope and duration. Scope refers to how widespread the event is. A cyberattack may affect just a few personal computers or many servers on a network. And the duration is how long the event lasts. A pandemic could affect people over 18 months or more, while a tornado might be over in minutes. As an information security example, many organizations are finding that data breaches started months before they were discovered. Note that scope and duration are independent variables. An incident may be of short duration but widespread in scope.

The occurrence of an event can be actual, in that it is in progress or has taken place. Or the event may be only potential, such as an approaching hurricane, or a warning that a new cyberexploit has been created. For potential incidents, the organization may have time to take precautions.

Onset is another characteristic, and it may be sudden or gradual. A sudden onset would be a fire breaking out or perhaps a cyberexploit. Gradual onsets may be due to inattention to preventive maintenance or low-level erosion or accumulations.

Perceptibility is the last characteristic. An event may be immediately noticeable and thus fairly easy to classify. Examples might be a fire or an unexpected system shutdown. Or it may be hard to discern: “Do I smell fumes?” “Hmm, there was an increase in calls to the help desk last week, even though many people are on vacation.” An event may be hard to perceive for a variety of reasons. Information may be incomplete, inaccurate, or contradictory. Or the threat may be “under the radar” if the events are small or even disaggregated. If an organization does not have a baseline of events that are considered normal, then it may have difficulty identifying events that are outliers. The outliers may be dismissed as flukes rather than taken as a trigger to act.

Organizations fail to see problems for a variety of reasons. Max Bazerman and Michael Watkins, in *Predictable Surprises*, list four areas of perception failures:

### Setting the telecom industry standard.

Read...

**Telecom Reseller**

IP-PBX/PBX • VOIP • SIP • SOFTWARE • SERVICE • MAINTENANCE • SPEECH • MOBILITY

THE NEWSPAPER for TELECOM NETWORKS

Visit www.telecomreseller.com & www.usernews.com

Tech Tips & Tricks • Buyer’s Guides To OEM Compatible Products • Professional Development & Training • Candid Advice & Views

ACUTA Members get free subscriptions. Please visit telecomreseller.com and hit subscribe.

Featuring

AvayaExtra • NEC Newslink • Inter-Tel Report • Nortel Now • Cisco IPT Tribune... and more
Figure 1. Sample Event Classification Scale

<table>
<thead>
<tr>
<th>Level</th>
<th>Impact Characteristics</th>
<th>Occurrence Potential/Actual</th>
<th>Information Quality</th>
<th>General Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Impact(s): None to low Scope, duration: Limited</td>
<td>Potential</td>
<td>Very uncertain</td>
<td>Wait and watch.</td>
</tr>
<tr>
<td>2</td>
<td>Impact(s): None to low Scope, duration: Limited</td>
<td>Potential or actual</td>
<td>Somewhat uncertain</td>
<td>Investigate, Plan possible responses, Alert managers of potentially impacted areas. Put teams on standby.</td>
</tr>
<tr>
<td>3</td>
<td>Impact(s): Low to moderate Scope/duration: Low to moderate</td>
<td>Potential or actual</td>
<td>Fairly certain</td>
<td>Pre-declare an incident. Notify management. Activate some teams. Set up incident command post.</td>
</tr>
<tr>
<td>5</td>
<td>Impact(s): Moderate to high Scope/duration: Moderate to high</td>
<td>Actual</td>
<td>Certain and confirmed</td>
<td>Notify management. Pre-declare a disaster.</td>
</tr>
</tbody>
</table>

- Scanning, through lack of attention or lack of resources;
- Integration, because people can’t “connect the dots”;
- Incentive, because no one thinks it is their responsibility to act or because acting would not be in someone’s interest; and
- Learning, where lessons have not been learned from previous incidents or the lessons have not been shared widely.

Information Security in More Detail

Confidentiality, integrity, and availability are critical aspects of information security.

Confidentiality applies not only to personal identifying information, but research information, financial information, and so on. A potential incident affecting confidentiality requires you to know the type(s) and quantity of data that are exposed. In addition, there are considerations of legal or other compliance requirements; these may be state data breach laws or the requirements of credit card companies under the Payment Card Industry Data Security Standard. Finally, consider whether aggregation of data elements, not necessarily all from a single source, can be of use to unauthorized persons obtaining that information. For example, identity thieves may obtain name, phone number, and address from one source and name and credit card number from another source.

For integrity, one factor is the criticality of the information, and this is based on the previous valuation of information assets during the risk analysis phase. Financial information, for example, is valued as more critical than addresses of vendors.

For both confidentiality and integrity, the scope and duration of the incident are also important. Was it a onetime event or continuing? Did someone mistakenly type a dollar amount, or is there a software bug that computes paychecks incorrectly (but only by pennies) week after week?

When availability is affected, questions of magnitude include the degree of service degradation and how many users or systems are affected. The criticality of the systems and the users affected by an outage or partial loss of availability must also be considered. The impact on availability can also be moderated if there are viable options for work-arounds, if only in the short term.

Finally, causative scenarios need to be taken into account, as these can have a bearing on response actions. For example, if an employee is responsible for loss of confidential information, then Human Resources will need to be notified. When information integrity is compromised, knowing the cause and whether the effect can be reproduced can be important. Detecting a rootkit will call for different actions than finding a software error.

Event Classification

After various characteristics of incidents have been identified, a classification system can be set up. The complexity of this system depends on its intended uses and audiences as well as the experience level of the organization and the resources it has to devote to the design.

Typical classification systems have from 3 to 12 categories on a scale. Examples would be hurricane classifications (category 1 through category 5) or the four-level medical emergency triage tag system (0 = expectant, 1 = immediate, 2 = delayed, 3 = minimal).

Impact is the key concept around which scales for hurricanes, tornadoes, earthquakes, and medical triage are built. The U.S. Coast Guard uses a different approach, based on information quality. The Coast Guard uses four classifications: nondistress (i.e., a vessel hasn’t returned to port when expected), uncertainty, alert, and distress (an S.O.S. has been received). Fairly simple classifications make them easy to understand, particularly in situations where time may be of the essence.

At the other extreme is a system used by the U.S. military that uses three-digit codes to classify situations. The first (or hundreds) digit identifies the broad category, with subcategories represented by the tens...
Thanks to Our Exhibitors and Sponsors!

Thanks to these companies that exhibited or sponsored at one, two, three or all four of our events in 2007, ACUTA members are their potential customers, but representatives from many of these companies have also become our partners in success as well as our friends. As they determine whose events they will attend each year, ACUTA is glad they have chosen ours.

<table>
<thead>
<tr>
<th>1 EVENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>3n (National Notification Network)</td>
</tr>
<tr>
<td>5G Wireless Communications, A1 Teletronic</td>
</tr>
<tr>
<td>Accu-Tech Corporation</td>
</tr>
<tr>
<td>Acentech Incorporated</td>
</tr>
<tr>
<td>Acentech Corporation</td>
</tr>
<tr>
<td>ADTRAN</td>
</tr>
<tr>
<td>AfTel Telecommunications</td>
</tr>
<tr>
<td>Alertus Technologies/Emergency AV</td>
</tr>
<tr>
<td>Bitn International</td>
</tr>
<tr>
<td>Blackberry</td>
</tr>
<tr>
<td>Blondentongue Laboratories</td>
</tr>
<tr>
<td>BlueNote Networks</td>
</tr>
<tr>
<td>Bradford Networks</td>
</tr>
<tr>
<td>CECECO</td>
</tr>
<tr>
<td>CheckPhone</td>
</tr>
<tr>
<td>Circa Telecom</td>
</tr>
<tr>
<td>Code Blue Corporation</td>
</tr>
<tr>
<td>Connect-ED</td>
</tr>
<tr>
<td>Convergent Systems</td>
</tr>
<tr>
<td>Corning Cable Systems</td>
</tr>
<tr>
<td>Cortelco</td>
</tr>
<tr>
<td>CosmoCom</td>
</tr>
<tr>
<td>Coyote Point Systems</td>
</tr>
<tr>
<td>Crescent Datacomm</td>
</tr>
<tr>
<td>Cross</td>
</tr>
<tr>
<td>Crown Castle International Corp.</td>
</tr>
<tr>
<td>Desire2Learn</td>
</tr>
<tr>
<td>Dymo Corporation</td>
</tr>
<tr>
<td>E2Campus</td>
</tr>
<tr>
<td>EchoStar Satellite, LLC</td>
</tr>
<tr>
<td>Embarq</td>
</tr>
<tr>
<td>FiberNet Telecom Group</td>
</tr>
<tr>
<td>Force10 Networks</td>
</tr>
<tr>
<td>Fujitsu Network Communications</td>
</tr>
<tr>
<td>G3 Technology Partners</td>
</tr>
<tr>
<td>GAI-Telefonic Corporation</td>
</tr>
<tr>
<td>Government Telecommunications</td>
</tr>
<tr>
<td>Graybar</td>
</tr>
<tr>
<td>Guardian Telecom</td>
</tr>
<tr>
<td>Hubbell Wiring Systems</td>
</tr>
<tr>
<td>Inspiron Logistics Corporation</td>
</tr>
<tr>
<td>ISI Telemanagement Solutions</td>
</tr>
<tr>
<td>Juniper Networks</td>
</tr>
<tr>
<td>Level 3 Communications</td>
</tr>
<tr>
<td>Maxcell Group</td>
</tr>
<tr>
<td>Meru Networks</td>
</tr>
<tr>
<td>MessageOne</td>
</tr>
<tr>
<td>MIR3</td>
</tr>
<tr>
<td>Mitel Networks</td>
</tr>
<tr>
<td>MobileSphere</td>
</tr>
<tr>
<td>Mohawk</td>
</tr>
<tr>
<td>Nuance Communications</td>
</tr>
<tr>
<td>Optus</td>
</tr>
<tr>
<td>PB Exchange</td>
</tr>
<tr>
<td>PertCell Plastics</td>
</tr>
<tr>
<td>Ramtel</td>
</tr>
<tr>
<td>Rave Wireless</td>
</tr>
<tr>
<td>RedSky Technologies</td>
</tr>
<tr>
<td>ReTele Communications</td>
</tr>
<tr>
<td>Ring Communications</td>
</tr>
<tr>
<td>SDC Solutions</td>
</tr>
<tr>
<td>SEI</td>
</tr>
<tr>
<td>ShipcomLab Communications</td>
</tr>
<tr>
<td>Siemens Communications</td>
</tr>
<tr>
<td>Snake Tray</td>
</tr>
<tr>
<td>SoTel Systems</td>
</tr>
<tr>
<td>Sumitomo Electric Lightwave</td>
</tr>
<tr>
<td>Superior Essex</td>
</tr>
<tr>
<td>TAC Centre</td>
</tr>
<tr>
<td>Talk-A-Phone Co.</td>
</tr>
<tr>
<td>Telesource Services, LLC</td>
</tr>
<tr>
<td>Telpro</td>
</tr>
<tr>
<td>ThinNic</td>
</tr>
<tr>
<td>United Data Technologies</td>
</tr>
<tr>
<td>USA Mobility</td>
</tr>
<tr>
<td>Video Furnace</td>
</tr>
<tr>
<td>Voice Mobility</td>
</tr>
<tr>
<td>VoicePlus</td>
</tr>
<tr>
<td>XTEND Communications Corp.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2 EVENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>5G Wireless Communications</td>
</tr>
<tr>
<td>Aastra Intecom</td>
</tr>
<tr>
<td>ADC</td>
</tr>
<tr>
<td>Alot Communications</td>
</tr>
<tr>
<td>Amcom Software</td>
</tr>
<tr>
<td>Anixter</td>
</tr>
<tr>
<td>Arbinet</td>
</tr>
<tr>
<td>AT&amp;T</td>
</tr>
<tr>
<td>Belden</td>
</tr>
<tr>
<td>Bluesocket</td>
</tr>
<tr>
<td>Campus TeleVideo</td>
</tr>
<tr>
<td>Carrier Access Corporation</td>
</tr>
<tr>
<td>Cedar Point Communications</td>
</tr>
<tr>
<td>Ciena Corporation</td>
</tr>
<tr>
<td>D&amp;S Communications</td>
</tr>
<tr>
<td>Falls Earth Station</td>
</tr>
<tr>
<td>GBH Communications</td>
</tr>
<tr>
<td>GigaFin Networks</td>
</tr>
<tr>
<td>IntraPoint</td>
</tr>
<tr>
<td>Microsemi/PowerDsine</td>
</tr>
<tr>
<td>Mobile Campus</td>
</tr>
<tr>
<td>NEC Unified Solutions</td>
</tr>
<tr>
<td>National Outdoor Media Network</td>
</tr>
<tr>
<td>Sprint</td>
</tr>
<tr>
<td>T3 Telecom Software</td>
</tr>
<tr>
<td>TeleMatrix</td>
</tr>
<tr>
<td>Tier Technologies</td>
</tr>
<tr>
<td>TRCA</td>
</tr>
<tr>
<td>Vantage Technology Consulting Group</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3 EVENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>3Com Corporation</td>
</tr>
<tr>
<td>Citel</td>
</tr>
<tr>
<td>CommScope</td>
</tr>
<tr>
<td>CommuniTech Services</td>
</tr>
<tr>
<td>Mapcom Systems</td>
</tr>
<tr>
<td>Mutare Software</td>
</tr>
<tr>
<td>OutPost Sentinel</td>
</tr>
<tr>
<td>Parlance Corp.</td>
</tr>
<tr>
<td>ProCurve Networking By HP</td>
</tr>
<tr>
<td>Telecom Technology Resellers</td>
</tr>
<tr>
<td>Teltronics</td>
</tr>
<tr>
<td>T-Metrics</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>4 EVENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acentech</td>
</tr>
<tr>
<td>Acoustics</td>
</tr>
<tr>
<td>Compco</td>
</tr>
<tr>
<td>Professional Computing Resources Inc.</td>
</tr>
<tr>
<td>PCR</td>
</tr>
<tr>
<td>Public Telephone</td>
</tr>
<tr>
<td>Qwest</td>
</tr>
<tr>
<td>Spirit of Service</td>
</tr>
<tr>
<td>SS8 Networks</td>
</tr>
<tr>
<td>verizon business</td>
</tr>
<tr>
<td>WTC</td>
</tr>
</tbody>
</table>
Advertisers’ Index

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

* * *

**911 ETC**
Dave Ellis (623/882-6526)
1504 Hewitt Ave., Ste. 401, Everett, WA 98201
dellis@911etc.com
www.911etc.com

**1Call, A Division of AMTELCO**
S. Robert Blankenship
800/356-9148
4600 Curtin Dr., McKfarrand, WI 53558
info@1call.com
www.1call.com

**Aastra Intecom**
Tim Whittington (800/468-3266)
2811 Internet Blvd., Frisco, TX 75034
sales@aastaintecom.com
www.aastaintecom.com

**AVST**
Sue Urban
513-563-8650
info@avst.com
www.avst.com

**Blackberry**
Blackberry
519/887-7465
www.blackberry.com

**Data Management**
Mike Dulaney (319-373-7773)
5250 N. Park Pl., Ste. 210, Cedar Rapids, IA 52402
mdulaney@dbman.com
www.dbman.com

**Dees Communications**
Louis Champan (425/869-1963)
4103 148th Ave. NE, Redmond, WA 98052
sales@dees.com
www.dees.com

**Genesys**
West Gass (650/466-1054)
2001 Junipero Serra Blvd., Daly City, CA 94014
wgass@genesyslab.com
www.genesyslab.com

**Hyperline Systems**
Evgeni Sokolov (613/735-8500)
2212 Gladwin Crescent, Unit C2, Ottawa, Ontario K1B 5N1 Canada
evgeni@sokolovsystems.com
www.hyperline.com

**Micromax/PowereDine**
Phil Lipkowitz (931/755-6430)
534 Broad Hollow Rd., Ste. 350, Melville, NY 11747
philipkowitiz@micromax.com
www.micromax.com

**MCTA**
888/994-2227
515 N. Washington, Ste. 405, Saginaw, MI 48637
mcta@mctatech.org
www.mctatech.org

**MIR3**
Ken Dixon (858/724-1200)
3398 Carmel Mountain Rd., San Diego, CA 92121
ken.dixon@m3i.com
www.mir3.com

**PAETEC**
Rick Cunningham (800/760-5697)
600 Willowbrook Office Park, Fairport, NY 14450
rick.cunningham@paetec.com
www.paetec.com

**Professional Computing Resources, Inc.**
Dan Ross (616/554-0000)
4635 N. Breton Ct., Kentwood, MI 49508
sales@pcr.com
www.pcr.com

**Sprint**
Richard Marvin (972/405-3100)
5020 Riverside Dr., Irving, TX 75039 (Mailstop TXIVGM0301)
richard.marvin@sprint.com
www.sprint.com/education

**Talk-A-Phone**
Jerry Nussbaum (773/339-1100)
5013 N. Kedzie Ave., Chicago, IL 60625
jnussbaum@talkaphone.com
www.talkaphone.com

**Telecom Reseller Magazine**
Doug Green (360/260-9708)
17413 SE 22nd St., Vancouver, WA 98683
publisher@usernews.com
www.telecomreseller.com

**Telecom Technology Resellers**
Michael Forst (603/827-7100 - 800/527-9990)
440 Sovereign Ct., Ballwin, MO 63011
mforst@teltechresellers.com
www.teltechresellers.com

**Windstream Supply, Inc.**
Mark Ogilvy (678/361-8581)
13560 Morris Rd., Alpharetta, GA
marc.ogilvy@windstream.com
www.windstreamsupply.com

**WTC**
Ron Rutherford (213/689-5309)
801 So. Grand Ave., Ste. 700, Los Angeles, CA 90017
rrutherford@wth-nc.net
www.wtc-inc.net

For details about advertising in the ACUTA Journal, contact
Amy Burton, Manager, Membership Marketing and Corporate Relations
Phone: 859/278-3338  x240  e-mail: aburton@acuta.org
www.acuta.org
digit, and a specific type of situation by the ones digit.

Suppose we propose a six-level scale based on impact characteristics, probability of occurrence, and the degree of certainty of information. Besides these, the scale should also incorporate general response actions (see Figure 1). Note that this is just a sample classification. Different organizations have different levels of risk tolerance based on their cultures and the types of risk they face.

Depending on your organization’s standards, a single-impact characteristic may force classifying an event at a certain level. For example, if the scope of an event is very widespread (high), while the impacts and duration are all low to moderate, the classification of 5 may be warranted.

Figure 2 depicts another view of classification, using x and y axes for information quality and for impact/magnitude respectively. Disasters would fall into the upper quadrants, with impacts ranging from moderate to high, while incidents occupy the lower quadrants, having low to moderate impact. When information is certain, then the event would belong on the right side of the graph; when it is less certain, it would fall to the left.

Incident Response

The classification scale in Figure 1 presents general response actions for incidents and disasters. Detailed response actions will be needed for each event scenario. Each scenario should also incorporate the classification levels, because as an event proceeds, the situation may change. Good incident management uses a feedback loop.

First there is an initial assessment of the situation, and this information is analyzed. Based on the analysis, interventions are chosen and applied, such as activating certain response teams, which then follow prescribed procedures. As the teams respond, the situation is reassessed to determine if the interventions have been successful or not. If subsequent analysis shows that the situation does not improve or that new dangers have arisen, then additional interventions are applied. The Air Force has a similar feedback loop with an easy to remember acronym, OODA: Observe, Orient, Decide, Act. The principle associated with this Air Force feedback loop is that you can defeat an enemy if you are better and faster at executing the OODA loop. Your response will be more successful the better you are at gathering information, assessing it, and then applying the right resources.

Air Force pilots undergo intensive and regular training to achieve first-rate response skills. However, responses to incidents and disasters in many organizations are not always fully effective, whether because of poor planning and preparation or lack of training. There are other reasons for ineffective responses as well. One is that information may be incomplete, confusing, or conflicting; the last is true when multiple sources provide information. Also, people tend to underestimate either the severity of the situation, the amount of time needed to react or control the situation, or the resources needed for the response. And related to underestimation is excessive optimism that the situation can be controlled.

When It's Over

At some point, it will be time to move from response to recovery. The incident and disaster response plans should identify criteria for declaring the end to an incident or disaster. This should happen when the situation has been stabilized or the disruption has ended.

Even when the response to an incident or disaster is quite successful, organizations should capture lessons learned. Sometimes called after-action reviews, these sessions should be held fairly soon after the event, and the results need to be shared with all potential stakeholders. After-action reviews cover both what went well and what went wrong, without any blame attached. The areas to examine during an after-action review range from detection of the incident through incident response and manage-

Figure 2. Classifying disasters and incidents

<table>
<thead>
<tr>
<th>Impact, Magnitude</th>
<th>Information Quality</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Certain</td>
</tr>
<tr>
<td>Potential disaster</td>
<td>Disaster</td>
</tr>
<tr>
<td>Low</td>
<td>Uncertain</td>
</tr>
<tr>
<td>Potential incident</td>
<td>Incident</td>
</tr>
</tbody>
</table>

ACUTA Journal of Communications Technology in Higher Education Spring 2008 47
Disaster Planning and Managing Expectations

Disaster planning on college campuses has historically been under-funded and neglected. Sadly, it has taken recent tragedies to bring the need for comprehensive disaster planning into sharp focus. In an effort to meet society’s expectations and stave off litigation, campuswide alerting and notification systems for staff and students as well as communications interoperability with community first responders have received an infusion of funds and attention. Comprehensive systems and plans have been implemented and tested at campuses across the country. Telecommunications has figured prominently in these activities.

Meanwhile, individual, non-critical campus departments, newly awakened to the consequences of disasters on their operations, have been developing plans without involving the telecommunications department. As a consequence, many departmental disaster plans assume telecommunications support that you most likely haven’t heard about.

You face three challenges in disaster planning for telecommunications:

- Design and maintenance of reliable telephony systems and services
- Support for other departments’ disaster plans
- Support for the staff and community

For most users, the voice network is invisible. When the power goes out, what is the first thing people do? They pick up their phone to report the outage. Voice communications is assumed.

To deliver on this presumption, manufacturers and service providers have designed and installed amazingly reliable phone systems and services. And, you’ve done an excellent job in ensuring this reliability on your campus—redundancy where needed, UPS and generator backup, wiring closet power, switch redirect services, operator relocation plans, staffing, and so on. You’ve always done this well—it is what you do.

But what about the expectations of non-operations departments: the English department, student health, chaplain, business school? Have you read their disaster plans? Or for that matter, even the IT department. Have you noticed that they say things like “You will be contacted . . .” or “Call the emergency number” or “Contact your department head/supervisor . . .” There is probably also mention of relocating command/operations to an alternate site where it is assumed that telephone calls (and data networking) will be routed and facilities will be in place to receive those calls.

Many departments may not have plans, but I can guarantee that they have expectations! It is important that you learn what they are and work with all departments to define their objectives and help them understand what it will take to meet their expectations. Determining costs and presenting a realistic view of the options can be time consuming and frustrating. As soon as you start to explain how much a plan will cost, departments will say they can live without it. But, the expectation doesn’t go away!

Let’s take a simple example of a department that’s made the effort to develop their own disaster plan. They’ve decided that calls are to be forwarded to a cell phone in the event of a building evacuation. Will the system let them call forward to an outside number? How many calls are we talking about? Will the person receiving those calls be able to handle the volume? What happens when the cell phone battery dies? What if there’s a prolonged power outage and the cell tower battery dies, or the tower is overloaded and calls can’t go through?

A simple questionnaire can be developed to step departments through the things they must consider and help them identify what is truly important and what they’re willing to pay for. Shared resources implemented for campuswide disasters can also be used to support local needs cost-effectively. You can educate departments about these. Additional considerations such as dealing with false disasters and ending real ones need to be brought out as well.

Finally, and most unpredictably, disasters will generate a substantial amount of incoming and outgoing call traffic between the campus, the community, and concerned families. Central offices and PBXs have finite call-handling capacities. Emergency services and first responders are allocated bandwidth that further restricts access to the public network. Since many campuses are in rural locations and served by a single central office, voice communications can be severely impacted in a disaster. Planning alternatives to voice communications over the public telephone network is critical. This requires creativity, perhaps partnering with institutions in other locations. Even if you do everything else right, failing to provide adequate communications between the campus and the community in a disaster will undermine all your best efforts.

The university community and individual departments have very high expectations of communications capability in the event of a disaster. Yet, the telecommunications department is not made aware of many of these. Your job is to provide leadership and develop a complete understanding of what’s expected so that you can deliver on the eternal expectation that phone service will always be there. Harry Newton (Newton’s Telecom Dictionary) used to say, “Dial tone does not come from God,” to which I would add, “But most folks think it does.”

Janet Smith is principal of Janet L. F. Smith & Associates. Reach her at janet@jifsmithassociates.com.
PowerDsine® Midspans
Get an A+ on All Your Power over Ethernet Upgrades

Simple Fast Affordable

A Single Connection for Video, Data, Voice and Power.

PowerDsine® Midspans are the cost-effective way to upgrade your network with the latest PoE technology.

They can fit easily into your budget whether for IT, infrastructure or specific applications including IP phones, wireless LAN access points or IP security camera systems.

With PowerDsine Midspans there's no downtime, no need to replace existing switches. They're plug and play fast and enhance the investment you've already made in your network infrastructure.

PowerDsine engineers pioneered the technology and are driving next-generation industry standards. So you can be confident with PowerDsine that you'll rise to the top of the PoE upgrades class. Worry free.

PowerDsine Midspans: the simple, fast and affordable way to send voice, data, video and power over a single wire. See how easy at www.powerdsine.com.

PowerDsine PoE Systems are now a product line of Microsemi Corporation

© 2007 Microsemi Corporation
Connecting the 21st Century Campus

A New Chapter in Unified Communications

Clearspan™

THE FUTURE CONNECTED

One Network
One Partner
One Solution . . . Delivered

For more information, contact us at 1.800.468.3266 or visit us online at:
www.aastraclearspan.com/acuta0308