inside: Virginia Tech fallout: the messaging systems | Deploying IP-based interoperability | Next-Gen 911 systems

COPS MANAGE THE STREETS WITH LARGE-SCALE WIRELESS VIDEO

INQUIRING EYES
Talk as one.
From day-to-day operations to disaster response, Harris Unity™ delivers true interoperability.

The company that developed the world’s first full-spectrum land mobile radio brings you the next-generation Harris Unity™ XG-100 Multiband Radio. With frequency band coverage from 136 to 870 MHz, extended battery life, and full P25 compliance, it enables you to connect with responders from any agency, whether they’re on analog or digital. Wherever you are, whatever the operation, carry the one radio that unites the entire team.

To order, call 1-888-711-7295. For more on interoperability, visit www.talkasone.com/EM

To experience the Unity XG-100, visit booth #1150 at IWCE in Las Vegas, NV, on March 18-20, 2009.
*Contents*

**FEATURES**

26
Beyond Borders
An IP-based solution connects North Carolina and Virginia law enforcement agencies.

32
Next-Gen 911
Network-based approach enhances public safety applications in Charlotte County, Fla.

38
Virginia Tech Fallout
Are students lulled into a false sense of security with messaging systems?

48
Food Safety
Basic principles and practices for communicating effectively before, during and after a crisis.

20
Wireless Convergence
Technological advances spur growth of large-scale video surveillance networks.
On Duty
On BlackBerry

Ideal solutions to stay connected and responsive.

For more information visit
www.blackberry.com/gov

© 2009 Research In Motion Limited. All rights reserved. BlackBerry®, RIM®, Research In Motion®, Suretype®, SurePress™ and related trademarks, names and logos are the property of Research In Motion Limited and are registered and/or used in the U.S. and countries around the world.
Myth Busters: Interoperability
Interoperable technologies already exist. However, before implementing any of this technology, we must face a bigger issue: cultural differences.

The inside pages of this publication are printed on 80 percent de-inked recycled fiber.
Mission Critical?

Mission Ready 24/7.

SAIC introduces the Expandable Shelter System (ESS): modular, expandable, deployable and multi-functional. ESS allows you to tailor the system to meet your application. ESS is ideal for C4I, forensic labs, disaster response, MASH units, berthing, field kitchens and more. Basically, it is limited only by the imagination.

For detailed information go to www.saic.com and type “ESS” in the search field, or call Patrick Cameron at 757.962.8139.
Eric Holdeman
Contributing Writer
Holdeman is a principal with ICF International, and former emergency management director of King County, Wash., a Project Impact community.

Jim McKay
Editor
McKay also is the justice and public safety editor of Government Technology magazine. He has spent more than a decade as a writer, editor and contributing writer for publications, including The Fresno (Calif.) Bee, The Vacaville (Calif.) Reporter and The Ring magazine.

Janet Hamilton
Contributing Writer
Hamilton is the 911 coordinator of Charlotte County, Fla., and is responsible for coordinating and maintaining the county’s 911 system. During her tenure she helped deliver Phases I and II of wireless enhanced 911 services. Hamilton began her career with the sheriff’s office in January 1992.

Hilton Collins
Staff Writer
Collins is a staff writer for Government Technology magazine. He’s written extensively on IT security and work force issues. Prior to joining Government Technology, Collins wrote for the Davis (Calif.) Life Magazine on various subjects.

Tim L. Tinker
Contributing Writer
Tinker is a senior associate of Booz Allen Hamilton and a crisis and risk-communications expert. He is co-director of Booz Allen Hamilton’s Center of Excellence for Risk and Crisis Communications.

Jim McKay
Editor
McKay also is the justice and public safety editor of Government Technology magazine. He has spent more than a decade as a writer, editor and contributing writer for publications, including The Fresno (Calif.) Bee, The Vacaville (Calif.) Reporter and The Ring magazine.

Colin Whitmore
Contributing Writer
Whitmore was an emergency management consultant and EMS Commander for the Virginia Tech Rescue Squad on April 16, 2007, when the shootings took place.

Adam Stone
Contributing Writer
Stone is a journalist based in Maryland who covers business and technology. He’s a regular contributor to Government Technology and Emergency Management magazines.

Janet Hamilton
Contributing Writer
Hamilton is the 911 coordinator of Charlotte County, Fla., and is responsible for coordinating and maintaining the county’s 911 system. During her tenure she helped deliver Phases I and II of wireless enhanced 911 services. Hamilton began her career with the sheriff’s office in January 1992.

Hilton Collins
Staff Writer
Collins is a staff writer for Government Technology magazine. He’s written extensively on IT security and work force issues. Prior to joining Government Technology, Collins wrote for the Davis (Calif.) Life Magazine on various subjects.

Tim L. Tinker
Contributing Writer
Tinker is a senior associate of Booz Allen Hamilton and a crisis and risk-communications expert. He is co-director of Booz Allen Hamilton’s Center of Excellence for Risk and Crisis Communications.

Jim McKay
Editor
McKay also is the justice and public safety editor of Government Technology magazine. He has spent more than a decade as a writer, editor and contributing writer for publications, including The Fresno (Calif.) Bee, The Vacaville (Calif.) Reporter and The Ring magazine.

Colin Whitmore
Contributing Writer
Whitmore was an emergency management consultant and EMS Commander for the Virginia Tech Rescue Squad on April 16, 2007, when the shootings took place.

Adam Stone
Contributing Writer
Stone is a journalist based in Maryland who covers business and technology. He’s a regular contributor to Government Technology and Emergency Management magazines.

Janet Hamilton
Contributing Writer
Hamilton is the 911 coordinator of Charlotte County, Fla., and is responsible for coordinating and maintaining the county’s 911 system. During her tenure she helped deliver Phases I and II of wireless enhanced 911 services. Hamilton began her career with the sheriff’s office in January 1992.
We Make Credentials Work

FRAC  TWIC  CAC  PIV

Introducing v3 of the CoreStreet PIVMAN Solution

Your job: securing the perimeter. Individuals are streaming in to provide critical support, but you’ve never seen them before.

They look right, but are they legitimate? Are they trained?

The CoreStreet PIVMAN Solution allows you to check any government-issued FIPS 201 credential, confirm the bearer’s identity, role, associated privileges or attributes, and log all activity. Anytime. Anywhere.

No network connections. No pre-enrollment. Just grab a handheld and go!

Rock-solid First Responder identity verification solution for FRAC, TWIC, PIV and CAC cards. Operational even in power out and network down environments. Tested in several DHS FEMA demonstrations and deployed within numerous federal agencies and state first responder initiatives. Reimbursable under various DHS grant programs.

Available on a range of Windows-based handhelds and PCs.

To learn more about CoreStreet’s Identity & Access Management solutions visit www.corestreet.com/FRAC
The March/April issue of Emergency Management magazine is heavier on technology than previous issues and, thus, a common theme emerges from the stories. The cover story, Wireless Convergence, explores the technological advances that have spawned the deployment of large-scale surveillance systems across the country. A convergence of new technologies, the availability of homeland security grants and the availability of licensed 4.9 GHz spectrum for public safety created an ideal breeding ground for these larger wireless systems.

Beyond Borders is about local agencies in Virginia and North Carolina that are working to implement a permanent voice over Internet protocol-based solution that would link IP, non-IP and radio networks inside one system. The system would help during situations that police there find themselves in all too often: A suspect hightails across the state line, and communications between the states involves a less-than-ideal, time-consuming process.

Virginia Tech Fallout is a look at the advances college campuses have made to safeguard their students and faculty from tragedy, like the one that befell the Virginia Tech campus. Since the shooting at Virginia Tech, colleges have a multitude of choices when it comes to mass-notification systems. But if you read deeply into each of these stories, you find a caveat. It's something you've read before in this magazine and will continue to read: Usually when you get to the crux of the issue, it becomes a people problem. The technology is available in most cases, but it's not a silver bullet.

In Virginia Tech Fallout, the author cautions that just setting up a mass-notification system isn't enough. And in Beyond Borders, we read about a fantastic system that was held back until “radio people understood IP people.” Wireless Convergence explains the gifts of the technology, but cautions: These systems won't stop a criminal from committing a crime; the systems are only as good as the people monitoring them.

David Boyd spells it out in our online feature Myth Busters: "Some emergency response agencies remain rooted in turf battles that make collaboration nearly impossible, while other agencies simply don't consider collaboration in their planning. Without collaboration, interoperability can never occur. Command structures, procedures, protocols and shared agreements must be established among regional agencies for responders to provide swift, coordinated support during incidents."

So what's the common theme? It's not technology, it's people.
A fire drill is not a metaphor here. It’s a molten mess of brick, steel and flames with your name on it. In these extreme conditions, there’s no time for miscommunication.

Nextel Direct Connect® offers interoperability, so you can get whomever you need on the horn across the fastest national push-to-talk network connecting the world’s largest push-to-talk community. Firefighters, police and EMS work together, seamlessly integrating into existing dispatch centers. And GPS services let dispatchers know exactly where every department is at all times.

Nextel Direct Connect. Only on the Now Network.™

To see Nextel Direct Connect in action, go to sprint.com/nextel

“Fastest” claim based on initial call setup time. GPS: Requires GPS and Java-enabled phone. Environment may limit GPS location info. Coverage not available everywhere. Nextel National Network reaches over 214 million people. ©2008 Sprint. Sprint and the logo are trademarks of Sprint. MOTOROLA and the Stylized M Logo are registered in the U.S. Patent and Trademark Office. Other marks are the property of their respective owners.
In the News

A devastating ice storm coated Kentucky with ice and snow in January, killing at least 21 people and halting power to nearly half a million residents, according to a CNN report.

National Guard troops were deployed on door-to-door missions to check on families in areas hardest hit by what Gov. Steve Beshear called the worst natural disaster to hit Kentucky in modern history.

As many as 6,500 residents were forced out of their homes by the extreme conditions and moved into shelters across the state.

Photo by Stephen George/LEO Weekly
Rebounding

The Gulf Coast was hit hard in 2005, with seven hurricanes tearing through the region. Katrina was the devastating showstopper, causing an estimated $81 billion in damage.

Following the storm, Gulf Coast builders and civic authorities found themselves in the hole. Even before the hurricane, the local building trades were shorthanded. Now, with post-Katrina rebuilding work to do, there were nowhere near enough hands to go around. Entire neighborhoods languished.

“We wound up hiring people who weren’t trained, who certainly would not earn as much money, who would not be as productive or efficient,” said Fred McManus, vice president of The Shaw Group Inc., a Baton Rouge, La., engineering and construction company.

Things have changed for McManus, whose 27,000-person firm has been able to bring in more than 3,000 trained workers in recent months. The windfall of personnel came thanks to the Gulf Coast Workforce Development Initiative (GCWDI), a public-private partnership that has trained more than 20,000 workers in various construction skills.

The effort has helped fill the labor gap, making it possible to rebuild and renew the region.

Assembling the Team

GCWDI had its genesis in a 2005 meeting of the Business Roundtable, a captains-of-industry conclave of about 160 CEOs working for major organizations. The group conceived a program to be led by the Bechtel Corp. and DuPont that would work for major organizations. The group conceived a program to be led by the Bechtel Corp. and DuPont that would work to fill the labor gap.

Members agreed to pitch in $5 million in cash and in-kind services, as a monetary foundation to attract $25 million in public support. The U.S. Department of Labor added $5 million to the pot through its Pathways to Construction Employment Initiative. Louisiana added $15 million more. National emergency grants, community block grants and other sources also supported the effort.

Planners conceived a three-pronged approach for the initiative, which formally launched in spring 2006: recruitment into construction careers, training and job placement.

Promotion came through the GCWDI Web site, www.imgreat.org, and paid advertising. Local community colleges formed the backbone of the training component. Contractors, homebuilders, trade groups and others stepped up with job-placement initiatives.

Planners and educators worked closely with those companies that would be hiring. “We wanted to let them know what our class schedules are, when students would become available and how to find them,” said Tim Horst, GCWDI program manager. Job fairs give recent graduates the chance to interact directly with employers.

Calling All Hands

Rebuilding the Gulf Coast means developing the work force.
Forging Partnerships

In addition to its government sponsors, GCWDI has drawn support from the community.

Trade associations have played a role, for example, through the Roofing Industry Alliance for Progress, which donated $25,000 to the effort. The National Roofing Contractors Association also donated resources to produce a recruitment video and worked with GCWDI to include a roofing component in the program's curriculum.

The education community stepped up with extensive training programs. Mississippi Gulf Coast Community College, for instance, offers a range of four-week courses based on the National Center for Construction Education and Research curriculum.

The Mississippi Construction Education Foundation also played a role. “They were at the table with us from the very beginning, helping us develop those programs and identify the shortages of workers in the entire construction industry,” said Anna Faye Kelley-Winders, vice president of Mississippi Gulf Coast Community College. “You must have partners at the table who are aware of those regional and national trends.”

The short-course format, produced outside a college’s usual for-credit track, allows for innovation. “[It] has made a great deal of difference because it allows us to try new things, to change formats, to respond to a particular need on a moment’s notice,” Kelley-Winders said. “Because you are operating outside the credit rules and regulations, there are fewer barriers to starting a program, to do it at night, for example, or in a new format.”

To round out their participation, colleges held a job fair for recent trainees, sometimes once a week. In the Louisiana Community and Technical College System, these events typically are highly targeted, zeroing in on the skills of a graduating class.

“Employers know the profile of the existing students, and they know their own needs, so it can be done on an appropriate level and in an appropriate way,” said Jim Henderson, senior vice president for work force training and development, Louisiana Community and Technical College System.

Best Practices

As the initiative unfolded, planners and participating entities slowly created a picture of best practices, starting with ideas about marketing strategies and tactics. From the educators’ point of view, getting the word out was a crucial component in making the project work.

“Outreach and recruiting were critical to the success of the effort,” Henderson said. “While the schools themselves lacked the resources to promote the initiative on a large scale, GCWDI was able to reach out into markets we couldn’t, and they brought in expertise in crafting the message.”

Planners took care in developing their marketing plan. “We took baby steps; we didn’t really put a lot of money into any marketing plan. ‘We took baby steps, we didn’t really put a lot of money into any one thing,” Horst said. Eventually a mix of radio, billboard, newspaper and other forms of advertising formed the core of the outreach message.

Not every effort succeeded, though. The team tried to market to car races, but the results were disappointing. “When people go to an auto race or a football game their mind is on that event, and they aren’t too interested in talking about construction,” Horst said.

Simultaneously more grass-roots efforts were used to reach out to individuals and institutions. At Advantous Consulting in Baton Rouge, for example, GCWDI Community and Outreach Manager Tim Johnson addressed career fairs in the inner city and worked with the Greater Baton Rouge Christian Ministerial Alliance to connect with some 85 African-American churches.

“Outreach and recruiting was critical to the success of the effort. While the schools themselves lacked the resources to promote the initiative on a large scale, GCWDI was able to reach out into markets we couldn’t, and they brought in expertise in crafting the message.”

— Jim Henderson, senior vice president, work force training and development, Louisiana Community and Technical College System

“You think about the impact a church has on its community and the ability to touch young people’s lives. In some cases, the churches will act as a haven for people who have specific needs, are down on their luck, need some direction and some opportunities,” Johnson said.

Positive Outcomes

GCWDI set out to train up to 20,000 new construction workers to the apprentice level by the end of 2009. In fact, the effort hit 20,421 training completions, with another 685 students enrolled in training, by December 2008.

How did the program rocket past its original target? “The synergy of having a public-private partnership is really important,” Horst said. “The federal government, with its financial resources, along with the community colleges, with their on-the-ground training and instructors, and the participation of employers — it all forms a very solid basis upon which to build.”

More than just a jump-start to regional rebuilding efforts, GCWDI has improved the lives of thousands of people.

“We know of any number of people who were lacking resources, and now they are working as carpenters and electricians. It has really turned their lives around,” Horst said. “They can think about buying a home or first automobile, something they could not have done before. It has opened brand new doors and new opportunities.”

Training began in mid-2006 and continues throughout the region, with programs in Mississippi, Texas, Alabama and Louisiana.

[The text continues with more detailed information on the programs and outcomes.]
Document on Nuclear Detonation Released

THE HOMELAND SECURITY COUNCIL released a document on nuclear detonation in the United States. The purpose of the guide, Planning Guidance for Response to Nuclear Detonation, is to provide emergency planners with recommendations that are specific to nuclear detonation with the goal of preserving life. The target audience includes response planners, their leaders, elected officials, and a broad spectrum of emergency managers and planners. The document is available at www.fas.org/irp/threat/detonation.pdf.

Schools Activate ICS With 911 Call

COLORADO SCHOOLS CAN ACTIVATE their Incident Command Systems by calling 911 thanks to new technology developed by School SAFE Communications.

A 911 call will activate a campuswide radio communications network that links school staff with first responders arriving on the scene.

Schools traditionally respond to a crisis by calling 911 then waiting for first responders. With the new system, schools will be immediately connected to local first responders’ two-way radios.

The system eliminates the need for first responders to install and carry a second set of radios compatible with the schools’. In addition, the schools do not have to purchase the more expensive radios used by the first responders.
Miraculous Tales of Survival Following Tornado

EIGHT PEOPLE DIED in a rare winter tornado in Lone Grove, Okla., but there were some miraculous survival stories in this town of about 4,600, which lies approximately 100 miles south of Oklahoma City.

According to an Associated Press report, a family was taking refuge in a closet when the tornado blew off part of the residence’s roof and lifted a young girl into the air, threatening to carry her away before family members snatched her in midair. Another woman was found injured but alive under an overturned mobile home.

In northwest Oklahoma City, the tornado damaged several shopping centers, restaurants and an apartment complex where some residents used a futon mattress to barricade themselves into a walk-in closet. While they were in the closet, a large part of the complex’s roof was blown off.

Now Available: DHS Rail Car Incident Course

A NEW COURSE, AWR 147 RAIL CAR INCIDENT RESPONSE, is now available to all 50 states and five territories. The eight-hour, instructor-led course is an introduction to basic rail car design and construction features, as well as assessment strategies to help interpret damage to the rail cars in the event of a hazardous materials spill.

The course is designed to educate rural first responders, government administrators and emergency managers on freight rail car incidents involving hazardous materials. Last year, more than 7,000 rail car accidents and incidents occurred, of which 20 involved hazardous materials that required more than 5,000 people to evacuate. In the last five years, there have been more than 166 incidents involving hazardous materials, and most of them happened in rural America.

More information can be obtained by calling Jo Brosius at the Rural Domestic Preparedness Consortium at 859/622-6445 or visiting www.ruraltraining.org.
How did Arkansas break out of the stovepipe scenario, where agencies and jurisdictions don’t communicate? After 9/11 it was decided by a key group within our leadership to look at funding mechanisms and start moving forward with an interoperable communication system.

The [Arkansas] Department of Emergency Management conducted a survey. Through that, they asked the locals questions and got feedback from them to identify what they thought their priorities are. There are always so many priorities that exist. So we worked really hard to put together a committee that was representative of the people carrying the radios. Particularly with public safety, our goal was to listen to the people who carry the devices.

How did you get all the stakeholders to the table? We recruited people who were recognized across the state for their leadership. In particular, we talked to our Association of Arkansas Counties and we reached out to our County Judges Association and the Emergency Management Association. From there, we asked them to nominate who they wanted on the steering committee.

We complemented that group with the technology group — that’s the group I represent. Then our director of security management, who is also the homeland security officer for the state, and representatives from the governor’s office, state police and [the technology group] formed the steering committee.

We’ve since grown that group because now we are out of that implementation phase and into the operational aspects of it.

We also engaged an independent quality assurance group that does not work for the state. We did a request for proposal to find one that specifically engineers radio systems across the nation, and I use that in a degree of risk mitigation because — from a state perspective, in the state-paid plan system — I cannot hire at the salary that would compensate for the level of individuals I would need that we could get for that quality-assurance group.

What hurdles did you have to sidestep during deployment? For many people, the system we had been investing in had not worked, in their minds, and didn’t support the state. So there was a lot of concern that we were going to create a new system and spend a lot of money on a technology that would not meet their needs. That made me realize how important it was to explain the differences between analog and digital to a live community of people who may or may not understand that process. We really had to make the system perform.
EVEN THE MOST SOLID FOUNDATIONS CAN BE SHAKEN...

L-3’s Risk Management Solutions provides the resiliency to prevent, protect, respond and recover.

L-3 Global Security & Engineering Solutions assists clients in developing all-hazards, scenario-based CON plans and OPS plans. We provide continuity of essential functions and services in the face of natural, technological, and man-made disasters, including terrorism. Our training and exercises are specifically tailored to our customers’ needs.

For additional information, please contact
Grant Peterson (703) 608-5259 or
Maya Chenault (703) 375-6543 or visit
L-3com.com/gses for more information.
Technological advances spur growth of large-scale video surveillance networks.
2008 may have been The Year of the Large-Scale Wireless Video Surveillance System, as several cities joined the growing market and others expanded existing systems. These systems stream high-resolution video to monitoring stations and police squad cars from cameras strategically located in downtown areas or other high-priority, high-crime districts. Cameras can prove valuable to police and prosecutors for capturing and convicting criminals and as a crime deterrent (and for managing large-scale events).

There are a few factors driving interest in these mostly hybrid fiber/wireless systems: a convergence of technological advances that lets jurisdictions build on existing infrastructure; the availability of licensed 4.9 GHz spectrum for public safety; and in some cases, the availability of homeland security grants to fund these projects.

Most recent deployments combine a fiber infrastructure with a mesh network, utilize multiradios (a radio accompanies each node on the system) and operate in the 4.9 GHz band — which was allocated for public safety by the FCC in 2002 to align with U.S. homeland security needs. The deployments capitalize on the shift from analog to Internet protocol (IP). Another key shift in the industry is that proprietary hardware systems are being replaced by software-based digital video management systems.

"The good news is that all the new pieces of technology come together in the systems, where it’s now open, standard, scalable; you can swap out any piece for any other piece," said Jasper Bruinzeel, vice president of marketing and sales for Wi4Net, a wireless broadband and video surveillance provider.
Hybrid Systems Grow Popular

Oklahoma City, Milwaukee, Long Beach, Calif.; Reading, Pa.; and Chicago have diverged into the market in a big way. Milwaukee’s system covers 97 square miles and has 15 cameras with more to be added later. The cameras stream real-time, high-resolution video to a centralized monitoring facility, where the video is stored for 120 days with 30 terabytes of storage. The storage is a direct-attached solution, which can expand as needed. Milwaukee’s video system is designed to scale to more than 100 cameras.

Hybrid systems provide the benefits of fiber without the costs of building a complete fiber infrastructure. For example, the city of Reading wrote an RFP for a fiber solution but instead opted for the hybrid developed by Wi4Net, according to Bruinzeel.

“The process, we said, ‘Wireless is available and has the ability to give a fiberlike experience if you design it right.’” Bruinzeel said. A 100 percent fiber solution wouldn’t have been cost-effective and wouldn’t have met expectations for video resolution and frame rate.

The hybrid solution can run at 30 frames per second at high resolution.

There isn’t a one-size-fits-all formula.

“It really depends on the city and what their expectations are,” Bruinzeel said. “In our Long Beach deployment, we’re expanding from 29 to 59 cameras and it all aggregates to a single aggregation point in 4.9 [GHz]. There is no fiber. To bring those 59 cameras all in one location, we’re running those streams at six to eight frames per second.”

That’s still a big improvement over the first-generation dual/single mesh radio approach that has limited capacity, Bruinzeel said. “You would never bring 59 cameras to one location [with dual/single radio], if you bring 10, you are doing well.”

Single- and dual-radio networks are subject to congestion as the number of network users increases. By contrast, multiple-radio network features a radio that accompanies each backhaul route, eliminating interference between nodes.

“Cloud” or network

In the future, Chicago could stream video into the mobile data terminals of 2,500 police cars. The city is planning for an aggressive crime analytics model to accompany the system, which makes the video quality critical. “You need to make sure you do it right the first time,” Argiropoulos said. “We’re using [mesh network provider] Fixiwire and finding in the 4.9 [GHz] license spectrum it’s some of the best in the industry in high-aggregate bandwidth.”

Chicago’s video is streamed to a control room at 30 frames per second of full-motion video from 1.2 megapixel cameras. The control room is staffed with 15 positions. Each
Inter-Government Crisis Network from Hughes

Connecting Government Leaders in a Crisis

What will you do if your terrestrial network goes down?

As a government leader, you need to coordinate decision-making among national, regional, and local levels to ensure maximum preparedness and rapid response when a crisis hits—which calls for highly reliable and resilient communications. But what happens if your terrestrial network fails?

Hughes has the ideal solution: The Inter-Government Crisis Network (IGCN). Operating over the Hughes SPACEWAY® 3 satellite system—the world’s first with on-board switching and routing, IGCN is secure, cost-effective, and instantly deployable. Unaffected by events on the ground, IGCN is immune to the vulnerabilities of the Internet and provides a true path diverse alternative to even the most robust terrestrial networks.

Frost & Sullivan recently released a whitepaper that discusses the critical issues in crisis communications, outlining a six-point summary of the key requirements for an ideal network to support effective decision-making among multiple levels of government agencies.

Contact Hughes for your copy of the Frost & Sullivan whitepaper and to learn how IGCN can help support your crisis management mission. Call 1-800-416-8679 or visit gov.hughes.com.

“New network provides spot-to-spot links that bypass all terrestrial infrastructure…”

William Jackson
Higher Level Communications
GCN, Jan 9, 2009

IGCN is available through SATCOM II, GSA Schedule 70, and Networx.
of them can talk to police units via a touchscreen radio system and generate a service call through the computer-aided dispatch system. The cameras are located at latitude and longitude coordinates and given a physical address. If there’s a disturbance near one of the cameras, staff can take a live look at the area and dispatch the nearest police unit.

“We have a 24/7 command and control room with a 28-foot video wall,” Argiropoulos said. “The room is set up like a battlefield, with video surveillance specialists sitting around in homeland security desks.”

The video is stored for 30 days with more than 90 terabytes of storage at a central location that’s replicated at a backup site.

Technological Advances

When a new Oklahoma City police officer arrives for his first day of work, his rank is entered into a computer system that automatically places him into the correct user group, which determines his access level to the citywide video surveillance system. Oklahoma City’s surveillance system covers 555 square miles — with nearly 500 cameras — and streams video to laptops in the police force’s 700 vehicles. When an event occurs, commanding officers who have the proper authority take control of the cameras nearest the incident and provide access to officers who are working the scene, controlling which cameras each officer sees.

Oklahoma City had big ideas when it first entertained the concept of a video-surveillance system about five years ago. City officials wanted a large-scale system that would be used by dozens of agencies and also structured hierarchically, so the appropriate people would have access to the appropriate cameras.

“Depending on how you do it, when you first entertained the concept of a video-surveillance system about five years ago, the city spent about $5 million on the system overall, but there were tremendous cost savings because of the ground-floor partnership with General Electric. ‘The concept [of the] meeting with General Electric was, ‘We will bring local expertise and help you develop this product and in return, you’re going to give us discounts on equipment, software and licensing.’ You have to have precise implementation plans,’ Meier said.

With nearly 500 cameras, it wasn’t feasible to put high-resolution cameras everywhere. The city looked for areas where real-time, high-quality video wasn’t necessary and used analog cameras in those places.

“A megapixel camera will pump through between 15 to 20 megabytes per second,” Meier said. “That’s a huge amount of data. We said, ‘We’re going to pump through a fraction of the amount of data. So by structuring it with different choices in different places to make the most effective use of the technology — and accepting that you can’t have this beautiful picture everywhere — you are able to reduce your costs significantly.’”

Oklahoma City chose to use the 2.4 GHz band instead of the 4.9 GHz band for this project, partly because of the deployment’s size, Meier said. “The density of the node placement is significantly lower for 2.4 and 4.9 does not get the penetration that 2.4 [does], so you need more infrastructure for 4.9. For an organization trying to cover almost 600 square miles with Wi-Fi, that is a very key point.”

The high cost and high expectations of a large-scale surveillance system — with few or no ways to measure return on investment (ROI) — makes it imperative that jurisdictions assess their needs and weigh them against the available options and costs.

“I see a lot of organizations that say, ‘We want this, and we’re going to take one approach to accomplish it,’” Meier said. “Well, you just drove up your costs phenomenally. It’s a relatively expensive system and unless you administrate it correctly, I’m concerned the value doesn’t meet the expectations.”

Measuring Success

These large-scale deployments are relatively new, and it’s hard to measure ROI. “How do you put a price on a life?” Argiropoulos asked.

The deployments can be a crime deterrent in some locations, and they can also be used for evidentiary purposes. “We’ve captured several crimes on video that have assisted in prosecution and also deterred a lot of internal affairs complaints,” said officer Eduardo Reyes, video camera administrator for the Long Beach Police Department. “Somebody says, ‘The officer punched me in the face.’ We look at it on video and nothing happened.”

Reyes said putting cameras everywhere wouldn’t necessarily work. “It has to be in certain spots, like the entertainment district. You have to weigh the benefits versus the costs.”
Seamless communication is vital when every second’s critical. You need a company that understands these demands.

Every day governments at every level are pressed to deliver their communities better public services. Services that are better coordinated. Services that save time, resources, and most importantly, lives. Fundamental to this effort are effective communication solutions. Alcatel-Lucent has years of public sector expertise in building mission critical communications networks. We know the demands. We know the pressures. We deliver those critical solutions. Visit us at http://www1.alcatel-lucent.com/us/slg. Or call 1-800-252-2835 and let’s work better together.

Transforming communications for a world that’s ALWAYS ON.

Alcatel-Lucent
IT'S THE TYPE OF NIGHTMARE that can raise a police officer's blood pressure: In the border region between Virginia and North Carolina, a suspect rockets down the highway so fast toward Pelham, N.C., that his car's speedometer creeps into the triple digits. Two Caswell County, N.C., officers follow behind as civilian vehicles swerve to avoid a collision. The suspect blasts through Pelham, and the officers see he's heading toward Danville, Va. They radio their county dispatch center, which in turn relays the message to Danville's dispatch — but then things go awry.

As the suspect crosses the state line, the North Carolina officers must end the pursuit because Virginia is not their jurisdiction. By the time Danville's dispatch notifies its police force and those officers are ready to engage, the suspect is gone. The two police forces' inability to seamlessly communicate enabled a criminal to avoid apprehension — an alarming problem that occurs when law enforcement agencies have radio systems that aren't integrated. This is problematic when a chase runs through multiple jurisdictions and affects multiple law enforcement agencies.

BY HILTON COLLINS
An IP-based solution connects North Carolina and Virginia law enforcement agencies.
"Pittsylvania County [Va.] surrounds Danville on three sides and also borders North Carolina, and the city of Danville borders North Carolina. And right across, sharing that same border is Caswell County [N.C]. There are at least two main thoroughfares that run between Virginia and North Carolina — highways 29 and 96,” said Maj. Dean Hairston of the Danville Police Department.

Many law enforcement and emergency management forces use land mobile radio technology to communicate, but often each agency has its own frequency and range — sufficient when talking among colleagues of a single department, but problematic for talking to other agencies. Sometimes a memorandum of understanding permits one agency to switch to another agency’s frequency if necessary. However, the drawback is an agency can’t use its own frequency while also using another jurisdiction’s frequency. In these cases, the long arm of the law can be thrown seriously out of joint.

But there’s hope on the horizon for regional authorities and their citizens.

Local agencies in Virginia and North Carolina are working to implement a permanent voice over Internet protocol (VoIP)-based solution that would link IP, non-IP and radio networks in one system. This would allow officers to talk across jurisdictional lines without ditching the equipment they’ve used for years.

The work toward this VoIP system began in 2005 with the Piedmont Regional Interoperability Project, a partnership between the city of Danville and Cisco Systems. The pilot was designed to determine how Cisco’s IP technology could assist authorities, and after reaching a promising 2007 proof-of-concept benchmark, officers and technicians are configuring the system for long-term use.

How It All Began

In 2005, Danville Police Chief Philip Broadfoot attended the International Association of Chiefs of Police conference and saw an eye-opening presentation by Cisco about the company’s IP Interoperability and Collaboration System (IPICS) technology. He was impressed that it integrated various modes of communication. IPICS had been tested in Honolulu and Miami, and Broadfoot figured that his region would make a great addition, so he approached Jeff Frazier, a director in the public-sector practice of Cisco Internet Business Solutions Group.

“They discussed the particular problems we were experiencing, and based on the increased level of deployment, Chief Broadfoot and Jeff [Frazier] both agreed that this would be a good fit for the third phase of product testing because it would allow them to use state agencies, county agencies and municipalities [together],” Hairston said.

That initial talk led to further discussion between Danville, Cisco and the National Institute of Justice (NIJ) — the research, development and evaluation agency of the U.S. Department of Justice. They wanted to know how IPICS could help jurisdictions in the Virginia-North Carolina border region communicate and collaborate, which led to the Piedmont Regional Interoperability Project’s creation. The project made Danville the host for frequency linkage between its own city, the Virginia State Police, North Carolina Highway...
Emergency Management

Patrol, Pittsylvania County Sheriff’s Office and the Caswell County Sheriff’s Office.

“We want to understand what role technology, in general, will play in that transition from analog to digital and what role Cisco may play in the analog-to-digital conversion,” Frazier said.

Cisco helped other regions make the analog-to-digital transition prior to the Piedmont project. A November 2005 Techworld.com article reported that IPICS was used in three deployments. After a two-week test in October 2005, the system improved communication between Honolulu police and fire departments and also the local government’s day-to-day operations.

Schiphol Telematics began testing IPICS in September 2005 in Amsterdam to evaluate its effectiveness for airport operations functions. Meanwhile, Maher Terminals began using it in June 2005 at a cargo terminal in Port Elizabeth, N.J., to give engineers a new way to deliver instructions to mechanics.

The Virginia-North Carolina partnership wanted its IPICS system to improve interagency collaboration and also save money in the long run. If the Piedmont project allowed agencies to communicate in a shared infrastructure with their existing landline phones, cell phones, radios and other handhelds, they wouldn’t be forced to pay for expensive upgrades to their land mobile radio or other equipment. According to Frazier, government public-safety departments in the rural United States could benefit financially from something like IPICS.

“A lot of these areas don’t have the money,” Frazier said. “They have a great need to collaborate, however, and radio over IP promises basic bridging and collaboration to give them, which is enormously important for them, he said.

Progress in Phases

By early 2006, Danville’s police, fire, emergency medical services, public works and city utilities departments were rolled into the first phase of the IPICS project. The second phase incorporated Pittsylvania County’s and Caswell County’s sheriffs, emergency medical services and fire departments. The third phase brought in the North Carolina and Virginia state highway patrols.

Cisco donated the routers for the project. In turn, Virginia granted $68,000 to the project to incorporate the Halifax County, N.C., Sheriff’s Office, which shares a joint emergency operations center with the South Boston Police Department of Virginia. The project also received some NIJ funding.

This connectivity and user functionality made for a successful test in 2007 that allowed law enforcement personnel to reach the proof-of-concept phase. But now that people know what they have, they must determine how to expand it and make it work best — hence, the reconfiguration.

“The system, for the most part, is a virtual system, meaning that you can access it from anywhere if you have IP connectivity,” Hairston said. “You can log on to the server, and you can create virtual talk groups if you’re authorized to do so.”

The IPICS server — located in Danville — supports communication between the jurisdictions. All frequencies are connected to a router that’s also connected to the server either by a T1, fiber optics or a microwave connection, Hairston said.

“This connectivity and user functionality made for a successful test in 2007 that allowed law enforcement personnel to reach the proof-of-concept phase. But now that people know what they have, they must determine how to expand it and make it work best — hence, the reconfiguration.” — Allan Sadowski, IT manager, North Carolina State Highway Patrol

“The Cisco people who came to the table on this were by and large [from a] voice-over-IP telephony background, and they came to the table and were talking with radio guys in a radio shop.”

“This deployment was a little bit different than what you see, say, in someone going out and purchasing because we did not have any

©ISTOCKPHOTO.COM/JOSEPH C. JUSTICE JR.

©ISTOCKPHOTO.COM/LISA F. YOUNG

100 Blue Ravine Road
Folsom, CA 95630
916-932-1300

PAGE
type of agreement. There was no maintenance contract," Hairston said. "Once you move to that phase and you start to look at, 'Well, hey, we want to use this system permanently,' you're talking about a brand new product. You're talking about the application of a number of different pieces of equipment, like routers, lines and things like that.'

For example, the jurisdictions must decide whether to continue using T1 lines for router connections, and if so, how they will pay for recurring costs. Any maintenance configurations or changes require infrastructure re-engineering, which takes time, cooperation and money. The jurisdictions also would like to connect the IPICS system to North Carolina's statewide radio system for emergency responders — VIPER, the Voice Interoperability Plan for Emergency Responders.

A Ways to Go

Although the IPICS system is functional, public safety officers aren't using it until there's a permanent setup. Some kinks still must be worked out, according to Allan Sadowski, the IT manager of the North Carolina State Highway Patrol.

Cisco initially projected six months to reach the proof-of-concept phase, he said, but in reality it took about two years. The officers had their day jobs and so did Cisco personnel. There was also some workplace culture shock between the two groups.

"The Cisco people who came to the table on this were by and large [from a] voice-over-IP telephony background, and they came to the table and were talking with radio guys in a radio shop," Sadowski said. Consequently there were some language barriers when it came to getting radio people to understand IP people, and vice versa.

The project's allure for Cisco, as Hairston sees it, was that it was an opportunity to learn how IPICS could work on top of a region's existing systems — some of which are outdated, and others cutting edge.

"So basically, they wanted to get the system up and running and make sure it was functional," Hairston said. "Once they had a proof-of-concept that we had communication, that we were testing and that we were able to communicate among the disparate systems, then they would come back and reconfigure the system for more permanent use."

The jurisdictions contracted with ARINC, a transportation communication and systems engineering solutions provider, to handle the system configuration.

"To be honest with you, I thought the system would have been up long before now," Hairston said. "I think it's a matter of, as soon as our attorneys and Cisco's attorneys have a final agreement, and we are able to issue the requisition for ARINC to come in and do the work. I suspect that in a very short period of time, we'll be up and running."

Had the jurisdictions gone the traditional RFP route instead of volunteering for testing, Hairston said the system would have been completed much sooner.

"At the end of the day, it'll be well worth it because we'll have a cutting-edge system and our basic cost on it will be minimal," he said. "Those are just some of the headaches that you kind of have to put up with."

New means of communication can affect the governance model when different jurisdictions work together for the same processes. IPICS is a bridge that links not only different forms of communication, Frazier said, but also different agencies in ways they've never been linked before. As a consequence, they can establish new modes of trust.

"We're not talking essentially about a technology, we're talking about a business change." — Jeff Frazier, director of public-sector practice, Cisco

Frazier said. "We're seeing IT change the governance structure."

"We're not talking essentially about a technology, we're talking about a business change." — Jeff Frazier, director of public-sector practice, Cisco

— Jeff Frazier, director of public-sector practice, Cisco
In recent years, the U.S. has faced a variety of costly natural and man-made disasters — from hurricanes, wildfires, floods and earthquakes to high-risk standoffs and the Sept. 11 terrorist attacks. These emergencies affect large numbers of citizens, amplifying the need for dependable communications among public safety organizations and emergency responders.

Many first responders rely on mobile phones to stay connected. But our nation’s terrestrial wireless infrastructure is both vulnerable to the congestion, damage or destruction that often occurs during emergency situations and inaccessible in many rural areas. Relying solely on these networks can leave public safety professionals and emergency responders disconnected when communication is needed the most.

Mobile communication challenges make it increasingly difficult for emergency responders to effectively coordinate and collaborate on rescue plans. This, ultimately, impacts response time.

“It is critical for us to be able to move rescue workers, medical support, repair teams and essential supplies in order to save lives and quickly begin recovery and rebuilding. And we can’t do that when our communication systems are down,” said Randy J. Johnson, assistant manager of communications for Plaquemines Parish in Louisiana, after experiencing the limitations of our nation’s terrestrial infrastructure during Hurricane Katrina.

To best serve and protect the public during emergencies and expedite decision making, government users of wireless communications require priority service on satellite systems, expanded coverage, redundancy and improved interoperability.

THE SMART™ SOLUTION

To ensure reliable interoperable communications, federal, state, local and tribal government and public safety agencies have joined nationwide and regional satellite-based mutual aid radio talkgroups (SMART). SMART is a program offered at no additional service and equipment cost to SkyTerra’s public safety users. Pioneered by the Department of Justice and the FBI, and operating on SkyTerra’s satellite network, the SMART program provides:

- Ubiquitous multi-state, multi-agency interoperable communications;
- A redundant communications system that allows public safety officials to stay connected during an emergency — even when terrestrial and cellular networks are damaged or congested;
- Expanded coverage, so that responders can communicate in the most rural and mountainous regions;
- Priority service for emergency response; and
- One-to-one “dispatch style” and one-to-many “broadcast style” push-to-talk communications.

By Adding SMART, we take fuller advantage of our existing equipment and greatly expand our ability to reach a broader cross section of public safety on a push-to-talk, one-to-many basis,” notes Robert Zanger of the Department of Justice Wireless Management Office.

The SMART program currently includes nine regional and nine nationwide talkgroups. The overlapping talkgroups enable critical and interoperable communications among homeland security officials, law enforcement, emergency responders and public safety teams across the nation.

With more than 3,300 users, SMART is proving to be invaluable for quickly and efficiently coordinating rescue efforts and providing the U.S. with a much-needed interoperable communications system. “The talkgroups provide a means of immediate communication between health and public safety professionals in and out of the state during an emergency,” noted Drew Chandler, IT and communications manager for The Kentucky Department of Public Health’s Preparedness Branch. The state of Kentucky made extensive use of its statewide network of satellite talkgroups during recovery operations following the devastating ice storms in the winter of 2009.

NEXT-GENERATION PUBLIC SAFETY INITIATIVES

The value of reliable, interoperable communication to the public safety community is greater now than ever. SkyTerra is in the advanced stages of building its next-generation, integrated satellite-terrestrial network, which will allow users to seamlessly and transparently toggle between cellular and satellite networks while still using a lightweight, handheld device. For public safety professionals, this means that the mobile device they rely on everyday could become the same device they reach for during an emergency. In addition, the dual satellite-terrestrial system will provide full redundancy and allow users to communicate from virtually anywhere across North America.

The Technology Council of the International Association of Fire Chiefs in cooperation with SkyTerra Communications recently developed an information paper that discusses the SMART program as a solution for nationwide interoperable communications. To download the information paper, visit www.iafc.org or www.skyterra.com.
Network-based approach enhances public safety applications in Charlotte County, Fla.

Visit any public safety agency in the United States and you are likely to witness the nation’s 911 network struggling to keep pace with citizen expectations and advances in communications technology. Public safety officials agree the move to the next generation of 911 is imperative.

However, as one Florida county learned, the public safety community must overcome many obstacles to successfully migrate to a next-generation 911 (NG911) system. These challenges include the integration of new applications into existing systems, developing new funding models, and addressing deployment and policy issues.

Charlotte County took on those obstacles and moved ahead with an NG911 system. There are two public safety answering points (PSAPs) in the county supporting one sheriff’s office, one police department, two fire departments and one medical response agency.
"Charlotte County moved forward with deploying a next-generation 911 network to better safeguard our citizens," said John Davenport, the county’s sheriff. "This new network will support traditional 911 operations, while also providing a secure foundation from which new lifesaving capabilities can grow — something our existing network can’t do."

"This new network will support traditional 911 operations while also providing a secure foundation from which new lifesaving capabilities can grow — something our existing network can’t do."

— John Davenport, sheriff, Charlotte County, Fla.

The Case for NG911

For the past 40 years, 911 operated as an overlay to the nation’s public switched telephone network, a circuit-switched network that provided the safe, secure and reliable operating environment that 911 required. New applications and system enhancements were built on this network, including the automatic delivery of callback numbers and locations, and continued improvements to call handling and computer-aided dispatch (CAD) capabilities.

More recently, 911 was required to receive wireless and IP-based 911 calls, forcing the network to provide 911 for communications technologies it wasn’t originally designed to support.

"New technologies have put a strain on the network and, in some cases, compromised the level of 911 service we can provide to our citizens," said Sherman Robinson, captain of the Charlotte County Sheriff’s Office. "With citizen expectations growing around the ability to send a text message or pictures to 911, or telematics-enabled [a combination of information and communications technology] vehicles to ‘call’ and transmit data to 911 in an accident, we are entering areas that the current network simply cannot accommodate."

Also, Charlotte County is frequently hit with severe weather. As with Hurricane Katrina in New Orleans and Charlotte County’s Hurricane...
Charley, survivability of the 911 network is essential regardless of Mother Nature’s force.

Building a Solid Foundation

For Charlotte County, a network-based approach to NG911 ensures survivability and addresses enhanced public safety applications like text messaging and dynamic routing of 911 calls during unpredictable emergency events. Rather than solely upgrading customer-premises equipment to IP — as in some public safety jurisdictions, which limits communicating outside of a 911 center’s operational footprint — Charlotte County officials recognized early on that a network-based approach would be the only way to fully realize NG911’s benefits.

Charlotte County has a much broader definition of NG911. The county’s new network will access both legacy and new IP-based capabilities.

Solving Funding Challenges

Funding for any government project is always an issue — now more than ever. Charlotte County’s funding challenge was somewhat mitigated because the costs associated with 911 services delivery were specified in existing tariffs defining what an enhanced-911 (E911) service provider can charge. As a result, the move to an NG911 network was a matter of shifting costs from the incumbent provider to Intrado Inc., the county’s new E911 service provider. Agreements between Charlotte County and Intrado were put into place for Intrado (through its regulated subsidiary, Intrado Communications) to deliver the 911 traffic from the county’s local-exchange carrier’s (LEC’s) central office. Once Charlotte County severed the relationship with the LEC, the Intrado Intelligent Emergency Network took over responsibility of routing all 911 call traffic.

Intrado is replacing the outdated, centralized, automatic message accounting trunks used by the previous service provider. This upgrade to the new IP-based network will handle all 911 call routing and delivery of automatic location information (ALI) for every 911 call, whether from a wireline, wireless or VoIP phone.

There were some incremental costs associated with the county’s decision to upgrade call-handling equipment. These costs were offset by reductions in monthly expenses for 911 services.
communication and equipment purchases that are necessary to maintain independent stand-alone PSAPs.

To cover the up-front costs, Charlotte County received a grant from the Florida 911 Board. Each of the state’s 67 counties was invited to participate in a competitive grant process for funds made available from wireless 911 fees.

“Charlotte County moved forward with deploying a next-generation 911 network to better safeguard our citizens.”

John Davenport, sheriff, Charlotte County, Fla.

Addressing Policy Issues

Currently the appropriate regulations and operational policies are in place for how 911 information may be requested by the public, how long 911 records must be archived and who can access 911 call data.

However, as the county moves beyond traditional technologies and begins to integrate text messaging, photos, video and telematics into the NG911 network, additional policy work is needed. Charlotte County is considering policy changes that would promote innovation in public safety networks and remove regulatory barriers that inhibit the deployment of new lifesaving applications and technologies. Such changes will help ensure that the county has access to the most progressive emergency services available in the market.

The Future of 911

Charlotte County has the technological foundation it needs to support its citizens’ current and future 911 needs, such as sending text messages or receiving telematics data from car crashes. In addition, the network-based model gives Charlotte County the operational flexibility to reroute 911 calls to help ensure that every 911 call gets the attention it needs.

Glossary

ANALOG: A representation of an object that resembles the original. Analog devices monitor conditions, such as movement, temperature and sound, and convert them into comparable electronic/mechanical patterns. For example, an analog watch represents the planet’s rotation with the rotating hands on the watch face.

DIGITAL: Traditionally it means the use of numbers and the term comes from digit or finger. Today, digital is synonymous with computer.

IP (INTERNET PROTOCOL): The part of TCP/IP that performs the addressing functions for networks.

NETWORK: An arrangement of devices that can communicate with each other.

PROTOCOL: The format and procedure that governs the transmitting and receiving of data.

PSAP (PUBLIC SAFETY ANSWERING POINT): A generic name for a municipal or county emergency communication center dispatch agency that directs 911 or other emergency calls to appropriate police, fire, and EMS agencies and personnel.

TELEMATICS: Originally coined to mean the convergence of telecommunications and information processing, this term later evolved to refer to automation in automobiles. GPS navigation, integrated hands-free cell phones, wireless communications and automatic driving assistance systems all come under the “telematics umbrella.”

TELEPHONY: "Sound over distance." It refers to electronically transmitting the human voice.

VoIP: Voice over Internet protocol. A telephone service that uses the Internet as a global telephone network.
The University of Connecticut is the first institution in the nation to offer a homeland security master’s degree program in partnership with the Naval Postgraduate School (NPS) in Monterey, CA.

- 2-year program prepares professionals to provide strategic leadership in fields with homeland security responsibilities.
- Emphasis on understanding the complexities of the homeland security arena in terms of policy, strategy, and organizational development issues.
- Provides graduates with a professional multi-disciplinary network of public and private sector leaders.
- Designed to meet the needs of working professionals: courses meet in-residence only four times and the remainder of the work is done online to accommodate each participant’s busy schedule.

Accepting applications now for Fall 2009. Deadline is July 1.

For more information, contact Donna Lee Campbell donna.campbell@uconn.edu or 860-486-0184.
April marks the second anniversary of the tragic shootings that took place on the Virginia Tech campus in Blacksburg. April 16, 2007, is a date that holds tragic significance to the students, staff, friends and family who feel connected to Virginia Tech. It was the day Seung-Hui Cho took the lives of 32 people in the worst mass shooting in U.S. history. It was a transformational day for the Virginia Tech community, but the shootings also shed light on the need for higher education to participate in emergency management in newer, more organized roles.

Virginia Gov. Tim Kaine appointed a panel of experts to review the incident and Virginia Tech's subsequent response. The panel made more than 70 recommendations, from mental health legislation to gun control laws to incident response policies.
The Virginia Tech campus was the backdrop for the worst mass shooting in U.S. history.
Any university official who read that report, no matter what institution they worked for, undoubtedly saw that significant work had to be done to prepare universities for an incident on the scale of the Virginia Tech shootings. Following the report’s release, universities scrambled to make changes to their emergency response plans. Most of them did their best to make changes that were visible to their communities. This sharply increased the demand for alert and warning systems, and there was a predictable surge in the number of companies offering them. Whether dealing with sirens, scrolling message boards or text messaging systems, it’s safe to say that nearly every U.S. university has installed or is installing a new messaging system for its campus.

Lulling Students

These installations, in many cases, have lulled students, staff and their families into a false sense of security. On a basic level, an inherent problem is that once an organization has the capability to send an emergency message, the organization still needs people who know what to say, when to say it and how to say it. Herein is the real problem with campus emergency management: Most colleges and universities still hesitate to address emergency management across all phases and make a real commitment to preparedness.

Nobody questions that there are daunting challenges when adopting emergency management best practices in an environment — higher education — that has never relied on them before. Universities are large and disparate organizations, with many departments seeking to fulfill their individual missions under the umbrella of a larger organization. Those departments face ever-shrinking budgets due to cuts at the state and federal levels. Concurrently they face growing student populations and increasing demands on their resources.

Understandably universities resist spending time and effort on planning for what most perceive to be highly unlikely — a man-made or natural disaster. Many of the nation’s larger universities, like Virginia Tech, resemble small cities — they are mostly independent communities with their own populations and even their own public safety agencies. One might compare the state of preparedness efforts at these universities to the state of preparedness in small cities before and immediately after the 9/11 attacks. However, colleges and universities have an advantage over small cities because they have best practices developed through years of other communities’ trials and errors that can be applied to their own emergency plans.

On one hand, the Virginia Tech shootings were a catalyst for colleges and universities to get serious about emergency management. It was easy to tune in to CNN or look at Facebook messages and see parallels between Virginia Tech and many other institutions. And because of the shocking and violent nature of the Virginia Tech incident, many institutions have focused their efforts primarily on security measures. But while the installation of central security offices, training of police officers, and the use of alert and warning systems are surely not a misallocation of resources, the problem remains that the institutions are largely unprepared to deal with a disaster when it occurs. These are the things that can only be learned through training and exercises.

Clearly some organizations have been quick to exercise their plans and procedures — as one might expect them to do. However, as we often see after any disaster, commitment to these efforts wanes as the political will to allocate funding diminishes as the sense of shock gradually decreases. Maintaining that commitment of...
<table>
<thead>
<tr>
<th>Institution</th>
<th>Program</th>
<th>Contact</th>
<th>Phone</th>
<th>E-Mail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adelphi University</td>
<td>Emergency Management Programs</td>
<td>Richard Rotanze</td>
<td>(516) 877-4552</td>
<td><a href="mailto:rotanz@adelphi.edu">rotanz@adelphi.edu</a></td>
</tr>
<tr>
<td>Arkansas Tech University</td>
<td>Emergency Administration and Management</td>
<td>Ed Leachman</td>
<td>(479) 964-0536</td>
<td><a href="mailto:eleaseham@atu.edu">eleaseham@atu.edu</a></td>
</tr>
<tr>
<td>American Public University</td>
<td>Emergency and Disaster Management</td>
<td>Chris Reynolds</td>
<td>(877) 777-9081</td>
<td><a href="mailto:creynolds@apus.edu">creynolds@apus.edu</a></td>
</tr>
<tr>
<td>California State University</td>
<td>Long Beach Professional Studies Department</td>
<td>Anthony Argott</td>
<td>(888) 999-9935</td>
<td><a href="mailto:aargott@csulb.edu">aargott@csulb.edu</a></td>
</tr>
<tr>
<td>Eastern Kentucky University</td>
<td>Master of Science in Safety, Security &amp; Emergency Management</td>
<td>Elizabeth Ballou</td>
<td>(859) 622-8325</td>
<td><a href="mailto:elizabeth.ballou@eku.edu">elizabeth.ballou@eku.edu</a></td>
</tr>
<tr>
<td>Eastern Michigan University</td>
<td>Department of Interdisciplinary Technology</td>
<td>Gerald Lawver</td>
<td>(734) 487-3170</td>
<td><a href="mailto:skip.lawver@emich.edu">skip.lawver@emich.edu</a></td>
</tr>
<tr>
<td>Elmira College</td>
<td>Master of Science in Emergency Preparedness</td>
<td>Angela Wood</td>
<td>(607) 735-1825</td>
<td><a href="mailto:awood@elmira.edu">awood@elmira.edu</a></td>
</tr>
<tr>
<td>Florida Atlantic University</td>
<td>Crisis &amp; Emergency Management Master of Business Administration Program</td>
<td>Martha Mehallis</td>
<td>(561) 297-0052</td>
<td><a href="mailto:mehallis@fau.edu">mehallis@fau.edu</a></td>
</tr>
<tr>
<td>Florida State University</td>
<td>Florida Public Affairs Center and the Center for Disaster Risk Policy</td>
<td>Janet D. Dileng</td>
<td>(850) 644-9961</td>
<td><a href="mailto:jdileng@florida.state.edu">jdileng@florida.state.edu</a></td>
</tr>
<tr>
<td>George Washington University</td>
<td>Institute for Crisis, Disaster and Risk Management</td>
<td>Gregory L. Shaw</td>
<td>(202) 994-6736</td>
<td><a href="mailto:gshaw@gwu.edu">gshaw@gwu.edu</a></td>
</tr>
<tr>
<td>Georgia State University</td>
<td>Master of Public Administration with a Concentration in Emergency Management</td>
<td>William L. Waugh Jr.</td>
<td>(404) 651-4592</td>
<td><a href="mailto:wwaugh@gsu.edu">wwaugh@gsu.edu</a></td>
</tr>
<tr>
<td>Jacksonville State University</td>
<td>Institute for Emergency Preparedness</td>
<td>Barry Cox</td>
<td>(602) 731-5291</td>
<td><a href="mailto:bc@jacksonville.edu">bc@jacksonville.edu</a></td>
</tr>
<tr>
<td>John Jay College, City University of New York</td>
<td>Master's Degree Concentration in Emergency Management</td>
<td>Norman Groner</td>
<td>(627) 237-8865</td>
<td><a href="mailto:ngroner@jjay.cuny.edu">ngroner@jjay.cuny.edu</a></td>
</tr>
<tr>
<td>Lynn University</td>
<td>Master of Science in Administration/Specialization in Emergency Planning</td>
<td>Ernest G. Vendrell</td>
<td>(561) 237-7446</td>
<td><a href="mailto:evendrell@lynn.edu">evendrell@lynn.edu</a></td>
</tr>
<tr>
<td>Louisiana State University</td>
<td>Disaster Science and Management</td>
<td>John C. Pine</td>
<td>(225) 578-1875</td>
<td><a href="mailto:jpine@lsu.edu">jpine@lsu.edu</a></td>
</tr>
<tr>
<td>Loma Linda University</td>
<td>Emergency Preparedness and Response Program</td>
<td>Ehren Ngo</td>
<td>(909) 558-8519</td>
<td><a href="mailto:engo@lsu.edu">engo@lsu.edu</a></td>
</tr>
<tr>
<td>Massachusetts Maritime Academy</td>
<td>Emergency Management and Facilities Management</td>
<td>Alfred Towle</td>
<td>(508) 830-5098</td>
<td><a href="mailto:atowle@massmaritime.edu">atowle@massmaritime.edu</a></td>
</tr>
<tr>
<td>Metropolitan College of New York</td>
<td>Emergency &amp; Disaster Management School of Public Affairs &amp; Administration</td>
<td>David Longshore</td>
<td>(646) 243-7608</td>
<td><a href="mailto:dlongshore@metropolitan.edu">dlongshore@metropolitan.edu</a></td>
</tr>
<tr>
<td>Millersville University</td>
<td>Master's Degree in Emergency Management</td>
<td>Henry W. Fischer</td>
<td>(717) 872-3568</td>
<td><a href="mailto:hfisher@millersville.edu">hfisher@millersville.edu</a></td>
</tr>
<tr>
<td>New Jersey Institute of Technology</td>
<td>Information Systems Department</td>
<td>Michael Chumer</td>
<td>(973) 596-5484</td>
<td><a href="mailto:mchumer@njit.edu">mchumer@njit.edu</a></td>
</tr>
<tr>
<td>New York Medical College, School of Public Health</td>
<td>Graduate Certificate in Emergency Preparedness</td>
<td>Michael Reilly</td>
<td>(914) 594-4919</td>
<td><a href="mailto:michael.reilly@nymc.edu">michael.reilly@nymc.edu</a></td>
</tr>
<tr>
<td>North Dakota State University</td>
<td>Master's Degree in Emergency Management</td>
<td>Daniel Kliewer</td>
<td>(701) 231-8925</td>
<td><a href="mailto:daniel.kliewer@ndsu.edu">daniel.kliewer@ndsu.edu</a></td>
</tr>
<tr>
<td>Northcentral University</td>
<td>Graduate Degree Programs with Homeland Security Specialization</td>
<td>Francisco C. Lopez</td>
<td>(807) 755-0839</td>
<td><a href="mailto:flopez@ncsu.edu">flopez@ncsu.edu</a></td>
</tr>
<tr>
<td>Norwich University</td>
<td>Master of Science in Business Continuity Management</td>
<td>John Orlando</td>
<td>(802) 485-2739</td>
<td><a href="mailto:jorlando@norwich.edu">jorlando@norwich.edu</a></td>
</tr>
<tr>
<td>Oklahoma State University</td>
<td>Master of Science in Fire and Emergency Management Administration</td>
<td>Anthony Brown</td>
<td>(405) 744-5606</td>
<td><a href="mailto:abrown@okstate.edu">abrown@okstate.edu</a></td>
</tr>
<tr>
<td>Olivet Nazarene University</td>
<td>Master of Science in Nursing Degree: Emergency Preparedness Disaster Readiness Track</td>
<td>Linda Davidson</td>
<td>(815) 939-5340</td>
<td><a href="mailto:ldavidson@olivet.edu">ldavidson@olivet.edu</a></td>
</tr>
<tr>
<td>Institution</td>
<td>Program</td>
<td>Contact</td>
<td>Phone</td>
<td>E-Mail</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>--------------------------------</td>
<td>------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>Park University</td>
<td>Disaster and Emergency Management Concentration</td>
<td>Laurie N. DiPadova-Stocks</td>
<td>(816) 423-1125</td>
<td><a href="mailto:ldipadovastocks@park.edu">ldipadovastocks@park.edu</a></td>
</tr>
<tr>
<td>Saint Louis University</td>
<td>Master of Science in Biosecurity and Disaster Preparedness</td>
<td>Larry Bommarito</td>
<td>(314) 977-8125</td>
<td><a href="mailto:lbommarit@slu.edu">lbommarit@slu.edu</a></td>
</tr>
<tr>
<td>Saint Xavier University</td>
<td>Graduate Certificate in Disaster Preparedness and Management</td>
<td>James C. Hagen</td>
<td>(708) 652-8220</td>
<td><a href="mailto:hagen@sxu.edu">hagen@sxu.edu</a></td>
</tr>
<tr>
<td>Texas A&amp;M University</td>
<td>Graduate Certificate in Environmental Hazard Management</td>
<td>Michael K. Lindell</td>
<td>(879) 862-3969</td>
<td><a href="mailto:mlindell@archone.tamu.edu">mlindell@archone.tamu.edu</a></td>
</tr>
<tr>
<td>University of Chicago</td>
<td>Master of Science in Threat and Response Management</td>
<td>Marsha Hawk</td>
<td>(773) 702-0460</td>
<td><a href="mailto:mhawk@uic.edu">mhawk@uic.edu</a></td>
</tr>
<tr>
<td>University of Colorado at Denver</td>
<td>Emergency Management and Homeland Security</td>
<td>Lloyd Burton</td>
<td>(303) 315-2482</td>
<td><a href="mailto:lburton@ucdenver.edu">lburton@ucdenver.edu</a></td>
</tr>
<tr>
<td>University of Connecticut</td>
<td>Masters of Professional Studies in Homeland Security</td>
<td>Donna Lee Campbell</td>
<td>(860) 486-0848</td>
<td><a href="mailto:dcampbell@uconn.edu">dcampbell@uconn.edu</a></td>
</tr>
<tr>
<td>University of Delaware</td>
<td>Master of Environmental and Energy Policy and Ph.D. in Environmental</td>
<td>Young-Doo Wang</td>
<td>(302) 831-8405</td>
<td><a href="mailto:ydmoon@udel.edu">ydmoon@udel.edu</a></td>
</tr>
<tr>
<td>University of Florida</td>
<td>Master of Science in Fire and Emergency Services</td>
<td>Barbara Klingensmith</td>
<td>(352) 369-2800</td>
<td><a href="mailto:klingenssmith@dfs.state.fl.us">klingenssmith@dfs.state.fl.us</a></td>
</tr>
<tr>
<td>University of Nevada at Las Vegas</td>
<td>Executive Master of Science in Crisis and Emergency Management Program</td>
<td>Christine G. Springer</td>
<td>(702) 895-4835</td>
<td><a href="mailto:christina.springer@unlv.edu">christina.springer@unlv.edu</a></td>
</tr>
<tr>
<td>University of New Orleans</td>
<td>Master of Public Administration with Hazard Policy Track</td>
<td>John J. Kierer</td>
<td>(504) 280-6457</td>
<td><a href="mailto:jkierer@uno.edu">jkierer@uno.edu</a></td>
</tr>
<tr>
<td>University of North Carolina at Chapel Hill</td>
<td>Master of Science in Disaster Management</td>
<td>Jim Porto</td>
<td>(919) 966-7354</td>
<td><a href="mailto:jim.porto@unc.edu">jim.porto@unc.edu</a></td>
</tr>
<tr>
<td>University of North Carolina at Charlotte</td>
<td>Master of Public Administration with Emergency Management Concentration</td>
<td>James W. Douglas</td>
<td>(704) 687-4532</td>
<td><a href="mailto:jwdouglas@unc.edu">jwdouglas@unc.edu</a></td>
</tr>
<tr>
<td>University of North Carolina at Pembroke</td>
<td>Emergency Management Master of Public Administration Concentration</td>
<td>Nicholas Giannatasis</td>
<td>(919) 521-6531</td>
<td><a href="mailto:giannatasis@uncp.edu">giannatasis@uncp.edu</a></td>
</tr>
<tr>
<td>University of North Texas</td>
<td>Master of Public Administration with Specialization in Emergency Administration and Planning</td>
<td>Bob Bland</td>
<td>(940) 565-2865</td>
<td><a href="mailto:mbland@unt.edu">mbland@unt.edu</a></td>
</tr>
<tr>
<td>University of Richmond</td>
<td>Master of Disaster Science Degree, Online (Thesis Track)</td>
<td>Leigh Anne Giblin</td>
<td>(804) 287-6837</td>
<td><a href="mailto:lgiblin@richmond.edu">lgiblin@richmond.edu</a></td>
</tr>
<tr>
<td>University of South Florida, College of Public Health</td>
<td>Graduate Certificate in Disaster Management</td>
<td>Wayne Westhoff</td>
<td>(813) 974-6625</td>
<td><a href="mailto:westhoff@hsc.usf.edu">westhoff@hsc.usf.edu</a></td>
</tr>
<tr>
<td>University of Tennessee, Knoxville</td>
<td>Emergency Management within Master’s Degree in Safety</td>
<td>Susan M. Smith</td>
<td>(865) 974-1108</td>
<td><a href="mailto:smithsm@utk.edu">smithsm@utk.edu</a></td>
</tr>
<tr>
<td>University of Washington</td>
<td>Institute for Hazard Mitigation Planning and Research</td>
<td>Bob Freitag</td>
<td>(206) 818-1175</td>
<td><a href="mailto:bfreitag@u.washington.edu">bfreitag@u.washington.edu</a></td>
</tr>
<tr>
<td>Virginia Commonwealth University</td>
<td>Master of Arts and Graduate Certificate in Homeland Security and Emergency Preparedness</td>
<td>John Aughenbaugh</td>
<td>(804) 828-8598</td>
<td><a href="mailto:jaughenbaugh@vcu.edu">jaughenbaugh@vcu.edu</a></td>
</tr>
<tr>
<td>Virginia Commonwealth University</td>
<td>Graduate Certificate in Homeland Security and Emergency Preparedness</td>
<td>Gregory L. Shaw</td>
<td>(804) 827-0879</td>
<td><a href="mailto:glshaw@vcu.edu">glshaw@vcu.edu</a></td>
</tr>
</tbody>
</table>
Homeland security concerns have created an urgent need for emergency management professionals in both government and private sectors. University of Maryland University College (UMUC) can prepare you for leadership in this rewarding career field.

- Convenient online and on-site classes
- Coursework will prepare you for professional certification in emergency management
- Scholarships, loans and an interest-free monthly payment plan available

Enroll now. Call 800-888-UMUC or visit umuc.edu/standup
College students are part of the community and should be included in planning disaster preparedness exercises.

Because colleges are unique among communities, they must recognize the need to include higher-education institutions as key planning partners when, in fact, a college and the community may face the reality, for the first time, of the need for coordinated planning and training. College administrators suddenly assigned these new responsibilities are frequently without direction. They haven’t been indoctrinated into the emergency management life cycle. (Survey a few college presidents on what the Incident Command System is if you’re not sure.)

Another interesting facet of U.S. campus preparedness is the increasing number of colleges and universities offering degrees in disciplines like disaster response, emergency management and homeland security. Some of the nation’s brightest, forward-thinking minds are spending their time and tuition to study the very challenges facing the universities where they study. This is undoubtedly the higher-education community’s most valuable resource for advancing preparedness. For example, a university that needs an updated emergency plan could likely find a Ph.D. student who’s eager to develop such a plan as part of a doctoral study. And a local college that’s addressing emergency management for the first time makes a remarkably valuable case study for the students of any emergency management degree program.

This vast resource of knowledge and manpower that’s being underutilized is a perfect example of the state of campus preparedness today. The need for university preparedness certainly exists, as was illustrated in April 2007 at Virginia Tech and again at Northern Illinois University in a February 2008 shooting that killed six. The knowledge gleaned from years of adapting best practices learned in every major U.S. disaster and the wisdom currently being taught in lecture halls exist separately. The creation of a reliable, consistent means of connecting the organizations in need with those that possess the knowledge remains an unmet goal.

U.S. colleges and universities — the higher-education community at large — exhibit all the characteristics of a community that’s forced to face the reality, for the first time, of the need for coordinated planning and training. College administrators suddenly assigned these new responsibilities are frequently without direction. They haven’t been indoctrinated into the emergency management life cycle. (Survey a few college presidents on what the Incident Command System is if you’re not sure.)

There’s little reason, two years after the Virginia Tech tragedy, for any college or university to be excluded from a community’s preparedness efforts. We must all equally share the responsibility of protecting and preparing the higher-education community through inclusion and open lines of communication. After all, that’s what coordinated preparedness is all about.
My education clearly sets me apart.

Specialized courses in emergency management and public law have helped me understand the complexities in Homeland Security/FEMA plans. As a result, my company more efficiently responds to those affected by devastation. The disaster management program certainly adds to my credibility.

Wayne Odachowski
Principal, Infinity Restoration
Student, Emergency and Disaster Management

Push your mind. Advance your career.

Join Wayne and 30,000 of his civilian and military classmates who are pursuing bachelor’s and master’s degrees online. Degree programs in fire science management, national security, emergency management, public administration, international relations, business, and more.

www.apus.edu or 877.777.9081

American Military University | American Public University
**Products**

**FM Alert**
Global Security Systems has teamed with Northrop Grumman Corp’s Mission Systems sector to deploy national, state and local alert and warning systems that use wireless and nonwireless communications infrastructure in consumer devices, such as cell phones, MP3 players and GPS devices.

The GSNNet Alert FM system uses an FM chip that can be inserted into many common consumer devices to enable them to receive alerts for weather, homeland security and local events, including traffic emergencies and Amber Alerts. The system has been installed in hundreds of FM radio stations and in at least 10 states across the Midwest and southeast. Visit www.alertfm.com for more information.

**Reverse 911**
The Reverse 911 Interactive Community Notification System is being used in thousands of communities, businesses and schools to improve the lines of communication to the general public and targeted groups.

Users can quickly target a precise geographic area and saturate it with thousands of calls per hour. The system's interactive technology provides immediate response to specific needs. Users can create a list of individuals with common characteristics to contact them with important information as needed. Visit www.reverse911.com for more information about the system and manufacturer PlantCML.

**Water Purification System**
The Self-Contained Water System by Global Waters Technologies is a water purification system for emergencies that's powered by a small gasoline engine and can function independently of an external power source. The SCWS-3000 is designed for fresh water, such as ponds, lakes and swimming pools. At 4 feet long, 2 feet high and 2 feet wide, it's storable and transportable. Visit www.globalwaterstec.com for more information.

**Marshals Deploy X-Ray Screening**
The U.S. Marshals Service will begin using advanced X-ray screening systems in courthouses across the country. The U.S. Marshals contracted with Smiths Detection for a $3.5 million deployment that will allow courthouses to screen for explosives and other threats in personal bags, briefcases and other belongings.

The HI-SCAN 6046i systems are used worldwide in airports, ports and border checkpoints, mass transit systems and first responder toolkits. See www.smithsdetection.com for more information.
THE COMPUTER FORENSICS SHOW
APRIL 27-29, 2009
WASHINGTON CONVENTION CENTER
WASHINGTON, DC

IMAGINE THE ABILITY TO VIEW ALMOST ANYTHING
THAT EVER APPEARED ON ANY COMPUTER

THE COMPUTER FORENSICS SHOW IS THE “MUST ATTEND” EVENT
OF THE YEAR FOR ALL LITIGATION, ACCOUNTING AND IT PROFESSIONALS

CONFERENCE DETAILS
MONDAY APRIL 27th: 3pm to 6pm
TUESDAY APRIL 28th: 9am to 6pm
WEDNESDAY APRIL 29th: 9am to 6pm

EXHIBITION HOURS
MONDAY APRIL 27th: 3pm to 6pm
TUESDAY APRIL 28th: 9am to 6pm
WEDNESDAY APRIL 29th: 9am to 6pm

For some companies, it is not a question if one of their computers will be used as evidence
in a legal matter, it is a question of when. Like it or not, every computer is a potential crime
scene and must be treated with care. When companies need to conduct internal investigations—
especially those involving litigation—discovering and maintaining evidence becomes paramount.

• Accountant Malpractice Claims
• Arbitration
• Broker/Dealer Claims
• Civil Litigation
• Class Action Disputes
• Construction Solutions
• Corporate Bankruptcy
• Corporate Governance
• Corporate Risk and Security
• Criminal Fraud & Deception Cases
• Employment Cases
• Family Law Cases
• Cyber Forensics
• Damage Assessment
• Digital Law
• E-Discovery
• Employee Internet Abuse
• Environmental Litigation
• Financial Investigations
• Forensic Accounting
• Industrial Espionage
• Insurance Claims
• Intellectual Property Claims
• International Risk & Investigations
• Intrusion Detection
• IT Security & Compliance
• Leasing & Derivatives
• Mergers & Acquisitions
• Post-Acquisition Disputes
• Disclosure of Corporate Information

PLEASE VISIT OUR WEBSITE AT WWW.COMPUTERFORENSICSHOW.COM

CONTACTS
Frank Manley, Show Director
94 Field Point Circle, Greenwich, CT 06870
Phone (203) 601-4312—Fax (203) 869.0283
fmanley@computerforensicshow.com

Ken Cardille, Sales Director
Phone (800) 767.2778
Fax (203) 869.0283
kcardille@computerforensicshow.com
**TAINTED TOMATO CASES REACH 552** was the headline of a June 20, 2008, MSNBC story. The Associated Press reported on Aug. 29, 2007, *Spinach Recalled Over Salmonella Fears*. This was preceded May 10, 2006, by another MSNBC story with the headline, *Toxic Pet Food Kills Dozens of Dogs*.

Though some of these stories were later proved inaccurate, these and other high-profile, food-safety crises vividly demonstrate how difficult it is to provide clear and consistent information to affected individuals, the professionals who come to their aid and the public at large. The communications of risk about these events were often inaccurate, inconsistent, inadequate or late. Communication missteps hampered community, state and national responses to the threats; in some cases, they resulted in widespread public confusion.
BASIC PRINCIPLES AND PRACTICES FOR COMMUNICATING EFFECTIVELY BEFORE, DURING AND AFTER A CRISIS.

FOOD SAFETY

BY TIM L. TINKER AND VINCENT T. COVELLO
These headlines speak to the challenges and perils of communicating to a public and media that demand immediate answers, scientific certainty and reassurances. Organizations that routinely monitor food-safety communications — such as Booz Allen Hamilton’s Food Safety Workgroup — note that during the 2007 bagged-spinach recall, federal public health authorities faced a communications dilemma. Although a single manufacturer was the target, it packaged spinach under several brands, which led to confusion and resistance about the recall. The result: Many consumers believed that no spinach was safe. More broadly, many avoided buying or eating not only spinach, but also a wide variety of green leafy produce.

In the case of the 2006 pet-food recall, initially federal authorities didn’t correctly identify the problem’s scope, which later impacted their credibility to the public and media. In fact, some authorities primarily reposted the manufacturers’ press releases, and consumers complained that they lacked correct or sufficient information about which products and manufacturers used the toxic ingredient. The steady stream of images and sound bites, as well as an online outcry from pet owners who lost their beloved animals only intensified the crisis.

These unintended consequences of food recalls and warnings illuminate the need for advanced planning, clear strategies, enhanced coordination and risk tools to effectively communicate with the public before, during and after food-safety defense crises. Research and experience show that the key to successful risk communication is for emergency management and public health systems to respond to public perceptions and to establish, maintain and increase their own credibility. The public must believe that government and commercial entities are working together and are in control of the situation. But most importantly, the public wants evidence that these entities have viable plans for early detection, rapid assessment and timely communications. They also want clear, accurate guidance on what the public should or shouldn’t do — e.g., “Do not eat food product X,” which might include specific identification guidance, or “Find a substitute.”

Vulnerability in Food-Safety Defense

In a December 2004 New York Times op-ed, Thaddeus C. Hill,iv Ed. Locally, Jennifer Wilkins, a food and society policy fellow in the Cornell Division of Nutritional Sciences, suggested the United States is particularly vulnerable to unintentional food-safety crises and intentional food-defense crises. She pointed to several factors that contribute to this vulnerability. For one, the United States is importing more food.

In a December 2004 Washington Times that half of the food consumed in the United States is imported. The Department of Health and Human Services estimates that less than 10 percent of imported foods are ever inspected. Moreover, contamination by food-borne diseases or a terrorist act doesn’t have to occur within the United States to have a devastating effect on the country’s food supply.

These factors may have been a priority for then-departing Health and Human Services Secretary Tommy Thompson when he publicly acknowledged the vulnerability of the U.S. food supply. In December 2004, Thompson said, “For the life of me, I cannot understand why the terrorists have not attacked our food supply because it is so easy to do.” Thompson was quoted similarly two months after the 9/11 attacks in a Time article. According to writer Frederick Golden, Thompson told Congress, “I am more fearful of this [organized attack on food and crops in North America] than anything else.” Whether the causes are intentional or unintentional, communicating about food-safety defense crises falls within the risk-communications parameters.

Risk-Communication Planning and Response

Numerous terms are used to describe risk, which can be confusing. The Presidential/ Congressional Commission on Risk Assessment and Risk Management’s 1997 final report refers to risk assessment as the process of organizing and evaluating information about the nature and strength of evidence, and likelihood of adverse health or ecological effects from one or a combination of threats. Risk management is the process of analyzing, selecting, implementing and evaluating actions to reduce risk. In this article, the term risk communication means the interactive exchange of information and opinion among individuals, groups and institutions about food-safety defense risk.

Risk communication is a science-based approach for communicating effectively in emotionally charged, high-stress or controversial situations. Also worth noting is the substantive growth in the last 20 years in the risk-communications body of knowledge. Still, risk communication continues to be a powerful, albeit neglected, tool for policymakers and emergency management professionals. A thorough understanding of the principles for risk-communication research and practice can inform and guide communication decision-makers in managing message content, messenger characteristics and channel effectiveness. The
Public safety professionals protect our communities in crisis situations and every day duty. It's not an easy job and the challenges are mounting. Understanding the key issues — from interoperable communications and security monitoring to business continuity planning — will get you on track to an optimum public safety strategy.

This comprehensive Guidebook identifies the full spectrum of public safety challenges, and offers recommendations and best practice checklists to help you solve these significant issues.

Now Available!

Leverage this insightful resource for training and development in your agency.

To receive your FREE copies, go to: www.govtech.com/publicsafety.
Perceptions of Risk

Leading risk-communication expert Peter Sandman identified at least 20 risk-perception or fear factors that can affect how concerned people view the magnitude of a food-safety defense risk, and therefore its acceptability. For example, risks are generally more worrisome, feared and less acceptable if they are perceived to be:

• under the control of others, especially if they aren’t trusted;
• involuntary;
• unfair or inequitable;
• man-made as opposed to natural in origin;
• unfamiliar or exotic;
• dreaded;
• uncertain; and
• a threat to children.

Risk-perception theory counters the conventional notion that facts speak for themselves. People commonly accept high risks, yet at the same time, they fear or become outraged over less-likely risks. For example, once a risk becomes familiar, it’s often less of a concern. In their perceptions research, noted risk-communication experts David Ropeik and Paul Slovic show that when bovine spongiform encephalopathy (BSE), known as mad cow disease, first appeared in Germany, a public opinion survey found that 85 percent of Germans thought it was a serious threat to public health. The same poll was conducted concurrently in the UK, where BSE had been around for years and had killed numerous animals and more than 100 people. The UK poll found that only 40 percent of British citizens considered BSE a serious threat.

More recently, in 2003, Steve Baake of The Denver Post and Matthews Walter of the Arkansas Democrat-Gazette reported on how the U.S. Department of Agriculture (USDA) announced a presumptive diagnosis of BSE in an adult Holstein cow in Washington state. Officials traced the animal’s origin to Canada using an ear tag identification number. The immediate fallout included a presumptive diagnosis before labs in England had verified the BSE. Second, despite a relatively low risk level to other livestock and human health, the agency publicly announced proposals to cut risk even further, including more testing, additional monitoring and tighter controls for imported cattle. These communications helped avoid a UK-style outbreak and more damaging impacts. According to the UK’s Department for Environment, Food and Rural Affairs, BSE affected 180,625 British cattle, and a virtual worldwide ban on British beef cost farmers billions of dollars.

Mental Noise

When people are severely stressed or concerned about a risk, their ability to process information is typically reduced by up to 80 percent. These concerns — “mental noise” — distract consumers and diminish their ability to effectively hear, understand and remember messages. Constructing and delivering information to a stressed population during a food-safety defense crisis is therefore radically different. Noted social scientist Elaine Vaughan points to possible negative consequences when risk-communication techniques and approaches aren’t appropriately applied, including:

• The audience is confused by the message.
• Strong reassurances are issued prematurely.
• Fears are raised without a simultaneous increase in self-efficacy or confidence in risk-reduction steps.
• Contradictory messages are sent.
• Public perceptions are ignored and concerns aren’t treated.
• The public refuses to follow recommendations.
• The public’s confidence declines in the assessment of risk by experts.
•friends accruing social and economic disruption.

Anticipation, Preparation and Practice

Planning is essential for successful risk communication about food-safety defense. Numerous communications experts advocate for risk-communication planning that employs specific techniques and approaches rather than generic program goals, is based on a working knowledge of the audience, provides a framework for addressing audience concerns, and most of all, is flexible. In addition, emergency management professionals must clearly understand the communication’s purpose, the audience and the fundamental message before engaging in risk communication.

Emergency management professionals first must know the purpose of the risk communication. The initial impetus of communicating food-safety defense risks is usually reactive. Is the goal to inform or persuade audiences? Each situation is unique, but with few exceptions, risk communication is used to assist individuals, communities and society at large to prevent, reduce or mitigate risk.

For risk communication to be effective, knowledge about the intended audience is also essential. One risk may have to be communicated to multiple audiences, including scientists, the general public, mass media, administrators, health-care professionals, private organizations or elected officials. Therefore, the communication must be tailored to the needs of each. It may also be necessary to use different channels to reach these various audiences. Moreover, the complexity and uncertainty of the scientific issues can mean that literacy and
Now more than ever,

IAEM is for you...

IAEM brings together emergency managers and disaster response professionals from all levels of government, as well as the military, the private sector, and volunteer organizations around the world.

- Largest expert network offering solutions, guidance and assistance.
- Job opportunities — extensive online compilation.
- Unified voice on policies and legislation.
- Information updates: monthly newsletter and e-mail notifications.
- Certified Emergency Manager® and Associate Emergency Manager programs.
- Scholarship program.

Join IAEM Today!

Save the Date
Oct. 31–Nov. 5, 2009

IAEM-USA 57th Annual Conference & EMEX 2009
Orange County Convention Center/
Rosen Centre Hotel
Orlando, Florida, USA
numerosity of audiences are especially important considerations.

The third element of risk communication is creating the message and preparing the messenger. Based on the science, purpose, audience and situation, emergency management professionals must decide on the main message to communicate. In risk communication, it could be that there’s little reason for concern, a great need for concern or that the potential risk is unknown. Planning is crucial in developing and using consistent messages. It’s important to recognize, however, that the risk-communication message may have to change over time because of the situation’s uncertainty and the possibility that new information will be discovered.

Effective risk communication about food-safety defense depends on the amount of work and detailed thinking that goes into planning and preparation before the crisis occurs. The more questions that can be asked and answered during this stage, the better the outcome will be. This is especially true regarding high-visibility issues, such as food-safety defense. The following are some sample questions developed by Booz Allen Hamilton’s Food Safety Workgroup:

✔ What do we want our risk communication to accomplish?
  • Increase collaboration with industry/growers to create a “cascading” communication effect with suppliers (grocery, wholesalers, food service) to increase message consistency and accuracy.
  • Proactively engage print, broadcast and electronic media by providing stories and amplifying messages through effective partnerships.
  • Harness and integrate the power of online media, such as blogs, webcasts and other electronic media, into one risk-communication plan.
  • Train representatives in the delivery of key messages.
  • Increase communication and information flow with manufacturers, distributors and retailers about sourcing, containing and limiting distribution of the product (food).
  • Communicate at the point-of-sale to get the prevention and mitigation message to consumers.

✔ What’s an optimal combination of strategies?
  • Establish a public Web site for accessing information, messages, materials, etc.
  • Assess which communication channels are most viable based on geography, type of product and type of consumer.
  • Gather and use historic data from previous recall efforts. When was it done well? Are there examples of when, how and why the public and food-supply chain reacted favorably or unfavorably (following guidance) to a recall?

✔ How can we assess progress and impact?
  • Conduct formative research and benchmark against best practice in risk communication.
  • Communicate lessons learned by monitoring media response; evaluating effectiveness of the messenger, message and

DIGNITY IN THE MIDST OF DISASTER.
The Everybody® Coffin provides response organizations with an alternative for managing mass fatalities by using a recognizable and traditional solution to a nontraditional problem. This unique coffin, with its patented, all natural wood design, allows for flat storage, assembly without tools and efficient stacking. For around $200, municipalities, hospitals and others now have an option when dealing with this public, yet personal issue.

For more information on the Everybody coffin please call 1-800-355-4628 or visit dqeredy.com/everybody

©2007 DQE, Inc.
Emergency Management

means; assessing risk-communication gaps and strengths; and making real-time adjustments when needed.

- Monitor blogs and other electronic media: What has the highest traffic and the most chatter (both positive and negative)?
- Analyze media placement and coverage and its implications for the overall risk-communication strategy.

✔ What's the real or perceived benefit if we execute our plan?

- Improve communication to strengthen reputation and credibility with consumers, industry, retailers, Congress, partners and other key stakeholders.
- Establish a communications presence in the market as the go-to source for information, updates and ongoing guidance.
- Use short- and long-term metrics to show the impacts of building ownership of the process with the target partner groups and progress on the food-protection plan.

Communicating food-safety defense risk is a complex endeavor with multiple perspectives, approaches and components. There's no single, standard food-safety defense situation or plan. The affected individuals may live close together or be scattered across the country. The type and extent of exposure, potential risks and possible actions that can be taken are highly variable. The best practices outlined in this article present a flexible, multicomponent approach for addressing the public's concerns, establishing trust and producing an informed public that's involved, interested, thoughtful, solution-oriented and collaborative.

These unintended consequences of a food crisis illuminate the need for advanced planning, clear strategies, enhanced coordination and risk tools to effectively communicate with the public before, during and after food-safety defense crises. Research and experience show that the key to successful risk communication is for emergency management and public health systems to respond to public perceptions and to establish, maintain and increase their own credibility and, therefore, the public's trust. This can be accomplished with advanced risk and crisis communication planning, clearly developed strategies and the development and implementation of communication tools and tactics to effectively reach the public before, during and after a food-safety or food-defense crisis.

✓ What’s the real or perceived benefit if we execute our plan?

- Improve communication to strengthen reputation and credibility with consumers, industry, retailers, Congress, partners and other key stakeholders.
- Establish a communications presence in the market as the go-to source for information, updates and ongoing guidance.
- Use short- and long-term metrics to show the impacts of building ownership of the process with the target partner groups and progress on the food-protection plan.

Communicating food-safety defense risk is a complex endeavor with multiple perspectives, approaches and components. There's no single, standard food-safety defense situation or plan. The affected individuals may live close together or be scattered across the country. The type and extent of exposure, potential risks and possible actions that can be taken are highly variable. The best practices outlined in this article present a flexible, multicomponent approach for addressing the public's concerns, establishing trust and producing an informed public that's involved, interested, thoughtful, solution-oriented and collaborative.

These unintended consequences of a food crisis illuminate the need for advanced planning, clear strategies, enhanced coordination and risk tools to effectively communicate with the public before, during and after food-safety defense crises. Research and experience show that the key to successful risk communication is for emergency management and public health systems to respond to public perceptions and to establish, maintain and increase their own credibility and, therefore, the public's trust. This can be accomplished with advanced risk and crisis communication planning, clearly developed strategies and the development and implementation of communication tools and tactics to effectively reach the public before, during and after a food-safety or food-defense crisis.
In government, many emergency management programs have moved around within a jurisdiction. Emergency management in King County, Wash., has moved from the sheriff’s office, to under the county executive and then to an administrative department. This movement in the program's placement isn't that unusual.

So where should the program reside? The "textbook solution" insists the best place is directly under the chief elected official. This way there's a personal connection and the weight of that office's authority to support the accomplishment of the necessary program elements during all phases of emergency management.

There are ups and downs to each option. This official may lack knowledge or not care about the emergency management function. Most elected officials live in the present; worrying about something that "might happen" isn't natural for them.

Another option is to create a special-purpose district that serves two or more jurisdictions. Some of these programs focus on specific aspects of the emergency management program, like planning and individual jurisdictions still coordinate response and recovery activities. There’s often a board of directors or some another group to oversee the program.

In reality, emergency management can function well in many circumstances. The key element is the leadership and support that are provided either by the elected official or through the parent organization's auspices. Remember that the grass or the funding isn't always greener on the other side of the org chart.
When the Interstate 35W bridge collapsed into the Mississippi River at 6:05 p.m. CST on Aug. 1, 2007, it took dozens of cars, trucks and other vehicles with it. Thirteen people were killed, and more than 80 injured drivers and passengers were thrown into a life-or-death situation. Trapped in the wreckage, many of those victims made the only call for help they could: They grabbed their cell phones and called 911.

Joining the ranks of our firefighters and police officers who saved many lives that day were those who worked in the Minneapolis Emergency Communications Center (MECC). Seconds after the bridge collapsed, MECC personnel began hearing from eyewitnesses and even victims who were still behind the wheel. The outstanding performance of the call center prompted the E911 Institute to recently award it “Outstanding Call Center” in 2008.

MECC’s 77-person staff answers around 660,000 calls annually. In the first two hours after the bridge collapse, the center handled three times the normal call volume. Along with calls coming in from the disaster site, the center heard from many who were concerned about loved ones. They also fielded calls from generous people who wanted to help. Despite this increased traffic, 911 operators and dispatchers managed to direct crews to the scene in just a few minutes.

MECC’s success did not come by chance. Preparations were made during prior years as part of Minneapolis’ overall emergency preparedness efforts. In disaster training, we found systems that worked and some that didn’t. We brought in new equipment and provided training when needed, and we were ready.

Just six months before the bridge collapse, MECC was equipped with a new computer-aided dispatch system. This technology let call center agents know where every Minneapolis’ emergency vehicle was located, and it helped them send additional crews where they were needed most. The computer-aided dispatch performed admirably during the bridge collapse, handling the heavy traffic without being overtaxed.

In addition, all MECC employees had done National Incident Management System and Incident Command System training. Among other things, this training provided them the know-how to work in an Incident Command System, which is a scalable framework that lets emergency responders from many different agencies work together effectively on disaster response.

But perhaps the greatest investment our city made involved upgrading its radio system to 800 MHz. Minneapolis and Hennepin County were pioneers in the Minneapolis metropolitan area by getting this technology into the hands of emergency personnel. These 800 MHz radios enabled the MECC to communicate with police and firefighters in the field, whether they were from Minneapolis or from one of dozens of other responding agencies. With the previous system, everyone talking at once on the radios made useful conversation difficult, if not impossible. This new radio system broke down the giant chatter into smaller groups based on tasks, which improved communications for everyone.

MECC’s performance has since been recognized as a model for other emergency call centers to follow. While I’m proud our dispatch center helped save so many lives when disaster struck, we don’t consider our work done. Emergency preparedness is an ongoing mission. Training and evaluation of our systems will keep taking place. We hope to never face another disaster like the one we did in 2007, but I know we’re doing the best we can to ensure we’re as ready as possible for the unexpected.
Talkgroups
Push-to-Talk
Emergency Response

Formerly Mobile Satellite Ventures

SkyTerra Communications
10802 Parkridge Boulevard, Reston, VA 20191-4334
Tel: +1 703 390 2700
www.skyterra.com
PREPARE FOR THE UNEXPECTED
WITH DELL DISASTER RECOVERY PLANS

BE PROACTIVE AND PROTECTED AT
DELL.COM/Recovery OR CALL 866.834.0156