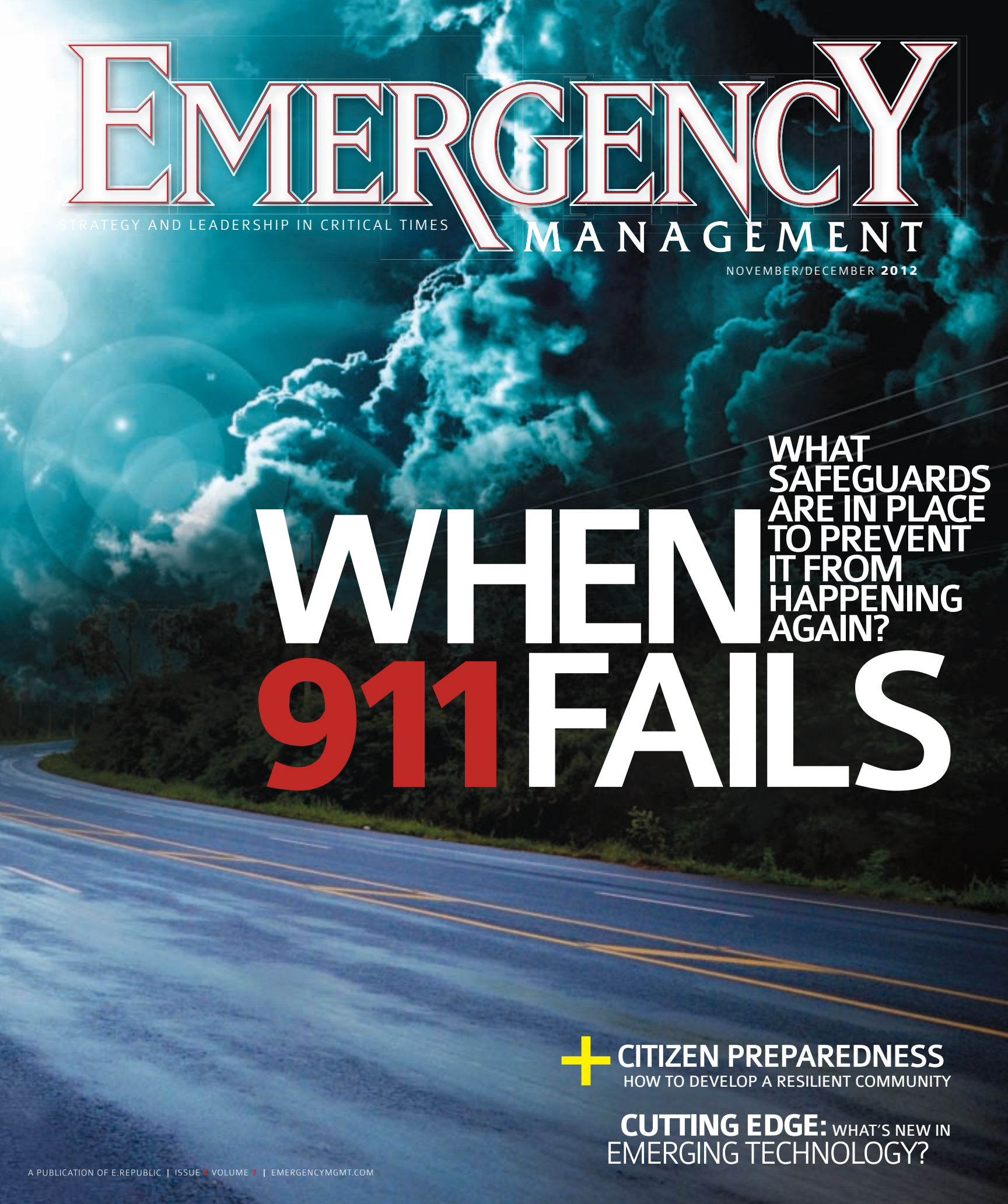


EMERGENCY MANAGEMENT

STRATEGY AND LEADERSHIP IN CRITICAL TIMES

NOVEMBER/DECEMBER 2012

WHEN 911 FAILS

WHAT SAFEGUARDS ARE IN PLACE TO PREVENT IT FROM HAPPENING AGAIN?

+ CITIZEN PREPAREDNESS
HOW TO DEVELOP A RESILIENT COMMUNITY

CUTTING EDGE: WHAT'S NEW IN EMERGING TECHNOLOGY?

A PUBLICATION OF E.REPUBLIC | ISSUE 6 VOLUME 7 | EMERGENCYMGMT.COM

Failure Is Not An Option!

Is your system's UP-TIME adequate?

Does your system limit in how many USERS it will allow?

Can you reach SUPPORT when you need them?

Does your system allow you to make DECISIONS instead of excuses?

Knowledge center™

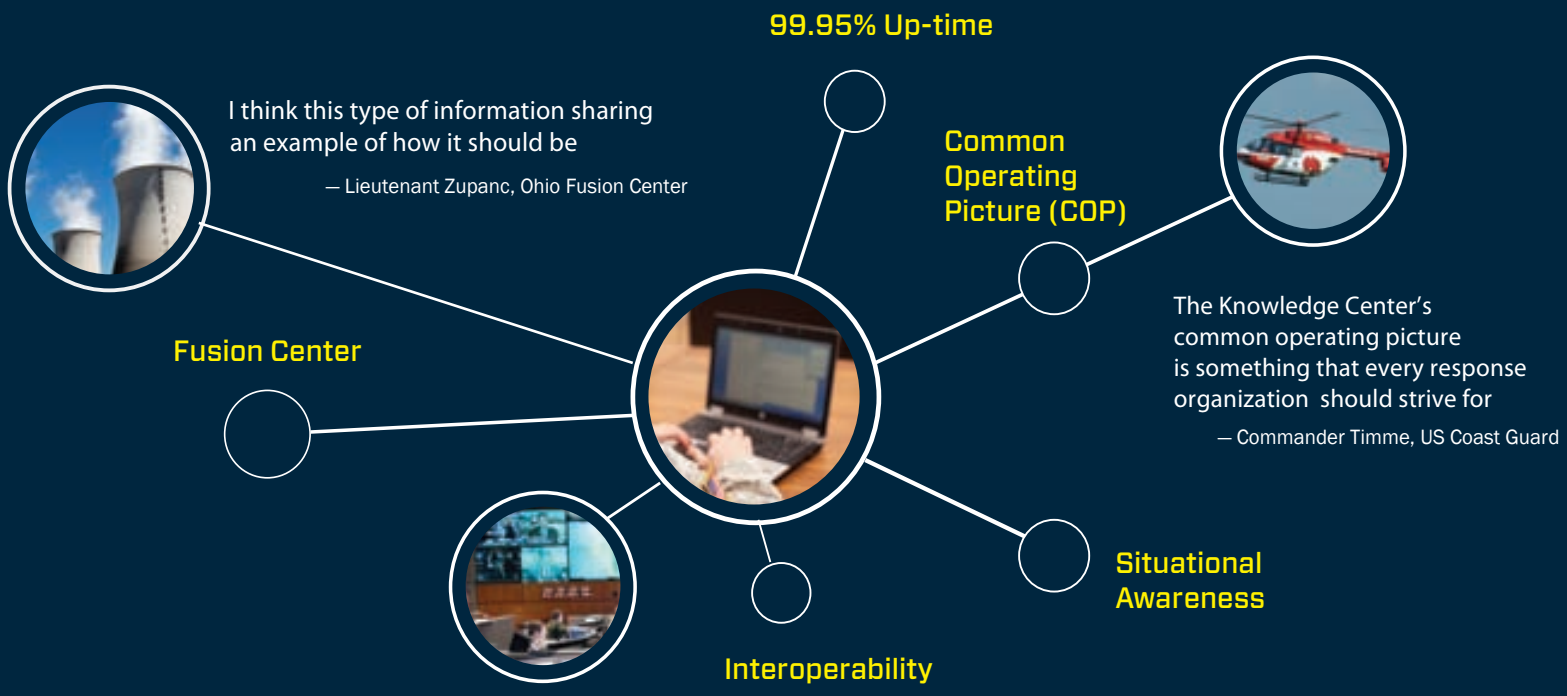
Incident Management Software Solutions



Call us : 412.635.3322

www.knowledge-center.com

Your team deserves a Best-of-Class solution, battle-tested for managing incidents and events.



Incident Management Software Solutions

Fully-functional, out-of-the-box, no training required.

Incident Management System

Incident Command System (ICS)
Critical Infrastructure/Key Resources (CI/KR)
Situation Reporting (SITREP)
Geographic Information Systems (GIS)

Hospital Incident Management System

Hospital Incident Command System (HICS)
Hazard Vulnerability Assessment (HVA)
Patient/Triage tracking
Hospital Available Beds (HAvBED)

Fusion System

Optimized intelligence sharing
Secure, tiered access control
Dynamic, configurable reporting
Interoperable with CADs

Knowledge Center™ is Proven



Contents

PHOTO COURTESY OF VIRGINIA DEPARTMENT OF TRANSPORTATION

FEATURES

Work anywhere, security everywhere.

AT&T has solutions to protect constituent data, no matter where it is – in a pocket, on a desk or dwelling in a data center.

State and local governments can count on AT&T's legendary reliability to provide both security and solutions to support and protect your agency.

Rethink how government does business inside the network of possibilities from AT&T.

To find out how, visit att.com/secureworkforce

VULNERABLE

PROTECTED

Rethink Possible®

Download the free scanner app at http://scan.mobi and scan this code to learn more.

Contents

SHUTTERSTOCK.COM

DEPARTMENTS

DISASTER RESPONSE

TRAINING AND EDUCATION

REST OF THE BOOK

VP Emergency Management/ Homeland Security: **Martin Pastula** mpastula@govtech.com (916) 932-1497

EDITORIAL

Editor: **Jim McKay** jmckay@govtech.com
Associate Editor: **Elaine Pittman** epittman@govtech.com
Managing Editor: **Karen Stewartson** kstewartson@govtech.com
Chief Copy Editor: **Miriam Jones** mjones@govtech.com
Contributing Editor: **Jessica B. Mulholland** jmulholland@govtech.com
Staff Writers: **Hilton Collins** hcollins@govtech.com
Brian Heaton bheaton@govtech.com
Noelle Knell nknell@govtech.com
Sarah Rich srich@govtech.com
Editorial Assistant: **Natalie August** naugust@govtech.com

DESIGN

Creative Director: **Kelly Martinelli** kmartinelli@govtech.com
Art Director: **Michelle Hamm** mhamm@govtech.com
Senior Designer: **Crystal Hopson** chopson@govtech.com
Illustrator: **Tom McKeith** tmckeith@govtech.com
Production Director: **Stephan Widmaier** swidm@govtech.com
Production Manager: production@govtech.com

PUBLISHING

VP Strategic Accounts: **Jon Fyffe** jfyffe@govtech.com
Stacy Ward-Probst sward@govtech.com
Chul Yim cyim@govtech.com
Leilani Cauthen lcauthen@govtech.com
Arlene Boeger aboeger@govtech.com
Sales Directors: **Leslie Hunter** lhunter@govtech.com
Shelley Ballard sballard@govtech.com
Liza Mendoza lmendoza@govtech.com
Kenny Hanson khanson@govtech.com
Tracy Meisler tmeisler@govtech.com
Kim Frame kframe@govtech.com
Account Executives: **Gloria Leacox** gleacox@govtech.com
Paul Dangberg pauld@govtech.com
Lara Roebbelen lroebbelen@govtech.com
David Rogers drogers@govtech.com
Account Managers: **Melissa Sellers** msellers@govtech.com
Erin Gross egross@govtech.com
Noel Hollis nhollis@govtech.com
Stephanie George sgeorge@govtech.com
Bus. Dev. Managers: **Glenn Swenson** gswenson@govtech.com
Maggie Ransier mransier@govtech.com
Sales Administrators: **Christine Childs** cchilds@govtech.com
Heather Woodhouse hwoodhouse@govtech.com
Carmen Mendoza cmendoza@govtech.com
Alexis Hart ahart@govtech.com
Dir. of Marketing: **Andrea Kleinbardt** akleinbardt@govtech.com
Dir. of Cust. Events: **Lana Herrera** lherrera@govtech.com
Dir. Custom Media: **Jeana Bruce** jbruce@govtech.com
Dir. of Web Marketing: **Zach Presnall** zpresnall@govtech.com
Web Advertising Mgr: **Julie Dedeaux** jdedeaux@govtech.com
Subscription Coord.: **Eenie Yang** subscriptions@govtech.com

CORPORATE

CEO: **Dennis McKenna** dmckenna@govtech.com
Executive VP: **Don Pearson** dpearson@govtech.com
Executive VP: **Cathilea Robinett** crobinet@centerdigitalgov.com
CAO: **Lisa Bernard** lbernard@govtech.com
CFO: **Paul Harney** pharney@govtech.com
VP of Events: **Alan Cox** acox@govtech.com
Chief Marketing Officer: **Margaret Mohr** mmohr@govtech.com
Chief Content Officer: **Paul W. Taylor** ptaylor@govtech.com

Emergency Management (ISSN 2156-2490) is published bimonthly by e.Republic Inc. 100 Blue Ravine Road, Folsom, CA 95630. Periodicals Postage paid at Folsom, CA and additional offices. Postmaster: Send address changes to Emergency Management 100 Blue Ravine Road, Folsom, CA 95630.

Article submissions should be sent to the attention of the Managing Editor. Reprints of all articles in this issue and past issues are available (500 minimum). Please direct inquiries for reprints and licensing to Wright's Media: (877) 652-5295, sales@wrightsmedia.com.

Subscription Information: Requests for subscriptions may be directed to subscription coordinator by phone or fax to the numbers below. You can also subscribe online at **www.emergencymgmt.com**

100 Blue Ravine Road, Folsom, CA 95630
Phone: (916)932-1300 Fax: (916)932-1470
www.emergencymgmt.com

A publication of e.Republic

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

GEORGETOWN UNIVERSITY

School *of* Continuing Studies

Earn your

Master's Degree in Emergency and Disaster Management

Gain the strategic skills required to head emergency management response efforts, improve public policy and, most importantly, save lives.

Learn from lifelike emergency management simulations, multi-location field study intensives and self-paced online studies.

To learn more, visit

SCS.GEORGETOWN.EDU/emermag

The *Left in Silence* article in the September/October issue struck a chord with many readers online in its discussion of how the deaf community is working at the grass-roots level to make progress in emergency management. Join the discussion at **www.emergencymgmt.com.**

I believe a special needs group that is being missed in all facets is the mentally challenged population, specifically autism spectrum disorders (ASD). This special-needs group is becoming an increasing population with one in 88 males being diagnosed on the autism spectrum. There are group homes that will need to be addressed, ASD college students and in the workforce [and] lastly ASD individuals living in personal homes without caretakers. When responders encounter individuals with ASD, the possibility of overlooking this disorder or not taking sufficient time to meet the needs of ASD individuals can cause the situation to escalate out of control. Responders need to be trained to first identify an ASD individual, be trained in strategies to deal with a situation and lastly have identifiable resources to manage the safety of the ASD individuals. In the fire service, we have had documented cases where an ASD individual has been removed from a house fire and the ASD individual has returned inside the home with tragic results. The potential is very great, that if ASD individuals or groups are not managed and secured, they will re-enter the emergency area. I think you offered some great information, but we as emergency responders are missing the largest growing special-needs population and we must always consider this population when dealing with future emergencies.
— Tim

The community of mentally challenged also presents unique difficulties in an emergency management situation. Many live alone with no access to social media and do not watch news or weather. It is important to know where these people are located and to have an appropriate means of notification that they can understand.
— Terri

It's important for communities to not fall short on making available a registry for the disabled. Not all have this yet, and even if they do, it is not always a user-friendly process. Some are forced to mail in the paperwork after printing it from the county website. And while Internet resources are stretched for some communities due to budgets, this process could be streamed down to an online registry. The next biggest issue is keeping that information secure and accurate, which greatly depends on the person with a disability to update their profiles every six months if need be, or whatever is an appropriate amount of time for a temp disability. At the very least, users should be required to update their profile once a year, or be dropped from the list. I have a disability as well, and I have worked in many disasters over the last two decades from coast to coast. Now I am forced to the side as my disability takes over.
— Chris

This article touches on important points but leaves out a lot of information. For starters, not one deaf individual was quoted or interviewed for this article. No disrespect is intended toward the efforts or Mr. Pope or Ms. Kent, but it's an insult to many of the outstanding individuals in this field who are working to achieve what the article states is an uphill battle. Moreover, there has been significant progress in the area at FEMA through the efforts of their Office of Disability Integration and Coordination. For starters, all of the videos under the 'Instructional Videos' tab at www.ready.gov/psa have ASL prominently featured.
— Neil

Statement of Ownership, Management and Circulation
(Required by 39 U.S.C. 3685)

Title of publication: Emergency Management. Publication No.: 5710. Date of filing October 1, 2012. Frequency of issue: Bimonthly No. of issues published annually: 6. Complete mailing address of known office of publication: 100 Blue Ravine Road, Folsom, CA 95630. Complete mailing address of general business offices of publisher: 100 Blue Ravine Road, Folsom, CA 95630. Full names and complete mailing addresses of publisher, editor and managing editor; Publisher: Don Pearson, 100 Blue Ravine Road, Folsom, CA 95630. Editor: Jim McKay, 100 Blue Ravine Road, Folsom CA 95630. Managing Editor: Karen Stewartson: 100 Blue Ravine Road, Folsom, CA 95630. Owner: e.Republic, Inc. dba Government Technology: Dennis McKenna and Robert Graves, 100 Blue Ravine Road, Folsom, CA 95630. Known bondholders, mortgages and other security holders owning 1 percent or more of the total amount of bonds, mortgages or other securities, none.

Extent and nature of Circulation		Average No. Copies Each Issue During Preceding 12 Months	No.Copies of Single Issue Published Nearest to Filing Date
A.	Total No. of copies	45615	45268
B.	Legitimate Paid and/or Requested Copies		
1.	Outside County Paid/Requested Mail Subscriptions Stated on PS Form 3541	29463	33152
2.	In-County Paid/Requested Mail Subscriptions stated on Form PS 3541	0	0
3.	Sales Through Dealers and Carriers, Street Vendors, Counter Sales, and Other Paid or Requested Distribution Outside USPS	0	0
4.	Requested Copies Distributed by Other Mail Classes Through the USPS	0	0
C.	Total Paid and/or Requested Circulation	29463	33152
D.	Nonrequested Distribution		
1.	Outside County Nonrequested Copies Stated on PS Form 3541	13111	9253
2.	In-County Nonrequested Copies Stated on PS Form 3541	0	0
3.	Nonrequested Copies Distributed Through the USPS by Other Classes of Mail	0	0
4.	Nonrequested Copies Distributed Outside the Mail	850	0
E.	Total Nonrequested Distribution	13961	9253
F.	Total Distribution	43424	42405
G.	Copies not Distributed	2191	2863
H.	Total	45615	45268
I.	Percent Paid and/or Requested Circulation	67.85%	78.18%

I certify that all information furnished on this form is true and complete.
Karen Stewartson, Managing Editor

Emergency Management Events

8-10 January

INTERNATIONAL DISASTER CONFERENCE & EXPO
New Orleans
IDCE unites public- and private-sector professionals worldwide for policy discussions and best practices.
www.internationaldisasterconference.com

15-17 January

UTILITY CYBER SECURITY & CIP COMPLIANCE
Atlanta
The conference focuses on balancing comprehensive security and grid requirements to minimize cyber-threats to utilities.
www.asdevents.com

Know the Situation

In an emergency, you need to understand what's happening now and what could happen next in order to make the best decisions. Esri® Technology provides you with comprehensive situational awareness and actionable intelligence when you need it most.

Learn more at esri.com/emmag

esri®

By Ian Torok

Talking Two-Way Radios

The narrowbanding mandate from the FCC has businesses and government entities working to retool their two-way radio systems in the face of stiff penalties and a Jan. 1, 2013, deadline.

The mandate states that all "Part 90" business, educational, industrial, public safety, and local and state government two-way radio system licensees currently operating legacy wideband (25 kHz) voice dispatch or data/supervisory control and data acquisition radio systems in the 150-174 MHz (VHF) and 421-512 MHz (UHF) bands must make the transition to the narrowband technology (12.5 kHz) by January.

The reason for the change is simple: The VHF and UHF land mobile radio bands are so congested that often there's not enough spectrum available for licensees to expand their systems or implement new ones. Requiring licensees to convert their radio systems to operate on narrower channel bandwidths will allow additional channels to exist within the same spectrum. Picture a four-lane highway jammed with traffic. If the road can't be widened, the only way to get more traffic on it is to make each lane narrower to make room for new lanes.

The urgency this year stems from the FCC's deadline and the likely penalties. Two-way radio users who don't make the switch face potential fines and possibly the loss of their communication capabilities.

For some, the task of reprogramming or replacing their older radios is so daunting that they are asking the FCC for waivers and extensions in order to avoid the stiff penalties for noncompliance. But waivers and extensions are far from automatic. And applying for an extension requires organizations to detail their narrowbanding efforts up to that point and commit to a new deadline.

Adding to the urgency is a rather complex and detailed conversion process that's been undertaken all over the country. It requires an assessment of the current equipment, the development of budget and funding options, the establishment of a conversion schedule, and the securing of a new or modified FCC license.

Most radios won't need to be replaced. Those purchased since 1998 may already have the ability to operate in both wide- and narrowband modes. They require only re-programming and re-licensing.

The latest two-way radios also offer an array of new features like texting, GPS capabilities and asset tracking that all lead to new levels of efficiency. And these days, applications aren't limited to smartphones. They're now widely available for two-way radios as well. Apps let organizations tailor radios to best meet their specific needs.

So while the FCC's narrowbanding update has caused some consternation, it also affords an opportunity to improve communications so businesses can be more efficient and people can be made safer.

Ian Torok is director of technical services for BearCom, a nationwide dealer and integrator of wireless communications equipment.

QUESTIONS OR COMMENTS?
PLEASE GIVE US YOUR INPUT BY CONTACTING OUR EDITORIAL DEPARTMENT AT EDITORIAL@EMERGENCYMGMT.COM, OR VISIT OUR WEBSITE AT WWW.EMERGENCYMGMT.COM.

Firefighting Protection

Emergency Response & Recovery

Law Enforcement & Security

Information Technology

Solutions That Save

Time, Money, and Lives.

Ensuring citizen safety and supporting critical business operations are important even during tough economic times. At GSA we offer direct access to a wide range of quality local and global contractors offering products and services at pre-negotiated ceiling prices. Our online tools and customer support specialists are available and ready to help you respond quickly to your state and local needs. GSA helps you generate efficiencies and savings for the American people.

To learn more, call **703-605-9155** or visit **www.gsa.gov/stateandlocal.**

GSA

U.S. General Services Administration

A car from a kiddie ride at Seaside Heights, N.J., boardwalk lies half buried in the sand of Mantoloking, N.J. — about 8 miles north of where it originated.

AP IMAGES.COM/WAYNE PARRY

In the News

As we went to press the death toll from Superstorm Sandy exceeded 175 and parts of the East Coast were still struggling with getting power back, finding fuel and a host of other issues.

Economists have estimated the cost of the disaster could be $30 billion to $50 billion in damages from individuals, businesses, insurers and the federal government expenses.

YOUNG GUNS

The federal government unveiled FEMA Corps in Vicksburg, Miss., on Sept. 19, inducting 240 enrollees into the emergency management program. FEMA Corps is a partnership between FEMA and the Corporation for National and Community Service that adds support for disaster response and recovery by new FEMA Corps teams within AmeriCorps. Each team consists of 10 FEMA Corps members, 18- to 24-year-olds who've signed up for the program.

"We're excited about the opportunity to bring more young people into emergency management to help serve the country," said FEMA Deputy Administrator Richard Serino. "They're going to eat, drink and live emergency management for 10 months."

FEMA Corps teams will support preparedness, response and recovery efforts by aiding survivors, helping with public communication efforts and more. The goal is to accumulate 1,600 FEMA Corps team members in the next 18 months, each serving 10 months with the option for a second year. The teams will respond to disasters anywhere in the country with the first teams heading to Louisiana and Mississippi to help with Hurricane Isaac recovery.

MARTY BAHAMONDE/FEMA

Post-Disaster Beer? Yes, Please!

A recently uncovered 1957 study says that beer (and other commercially packaged beverages) will be safe to drink after a nuclear explosion. NPR reported that the Atomic Energy Commission exploded two bombs at a Nevada test site with bottles and cans placed around ground zero, with the closest containers located less than a quarter mile away. The surviving bottles were checked for radiation, and while the bottles near ground zero were radioactive, their contents weren't, but the flavor was altered.

GLOBAL INITIATIVE

In October, the American Red Cross, with the International Federation of Red Cross and Red Crescent Societies, launched the Global Disaster Preparedness Center, a reference center to support learning and knowledge sharing for disaster preparedness practitioners. Initiatives that will be focused on in the next year include an interactive website that will foster learning, exchange of materials and networking. In addition, a research program will fund studies on topics like the value of social media in public awareness and cost benefit analysis of disaster preparedness interventions.

MOBILE PREP

Arkansas' Department of Emergency Management (ADEM) has logged thousands of downloads of its mobile app, Ready AR, since its September release. It features updated data on roadway and weather conditions, current threats and emergency planning.

"The state faces quite a few weather and natural disaster threats, including earthquakes, tornadoes [and] winter events," said Chad Stover, ADEM deputy public information officer. "The app is designed to give residents tools to be able to use to face those disasters."

Stover reports that other state agencies have approached ADEM hoping to add their preparedness resources to the app in a future update. Talks are ongoing to possibly add more law enforcement information and public health resources.

An alternative P25 solution is at hand.

As a radio communications manager the last thing you need is to be locked into an expensive and inflexible provider.

With 42 years of experience, Tait is a global leader in working with Public Safety agencies to build great mission critical communications solutions.

Our standards based and non-proprietary P25 platform gives you the flexibility to build better P25 networks that will exceed your expectations.

- End-to-end system design, manufacture and deployment
- Backed by world-class system support
- True P25 standards-based design
- Software upgradeable to P25 Phase 2
- CAP tested for interoperability
- Robust and reliable base stations, portables, and mobiles
- One of the most compact and lightweight P25-compliant portable radios on the market

For the complete solution visit **www.taitradio.com/P25**

tait communications

Tait P25. Engineered to exceed Public Safety's changing needs.

By Adam Stone

WHEN 911 FAILS

WHAT SAFEGUARDS ARE IN PLACE TO PREVENT IT FROM HAPPENING AGAIN?

People know what to do when they get into a car accident: Call 911. They know what to do when the traffic signals go out: Call 911. But what do you do when 911 goes out?

The question was more than merely academic for some 2.3 million residents in northern Virginia who lost telephone access to emergency services for up to four days in June in the wake of a quick and violent thunderstorm known as a derecho.

SHUTTERSTOCK.COM

Congress moved as swiftly as the derecho itself to express its displeasure with the 911 outage. In a letter to FCC Chairman Julius Genachowski, U.S. Reps. Jim Moran, Gerry Connolly and Frank Wolf wrote: "In the event of an emergency situation, whether it be a natural disaster or man-made threat, the public needs confidence that they can get through to 911 operators. This storm exposed a weakness in our response system, and now that we know it exists, we must fix it."

To fix it, you first have to understand it. With multiple investigations under way in Washington, *Emergency Management* asked Fairfax, County Director of Public Safety Communications Steve Souder to describe the events surrounding the 911 blackout.

It was the evening of June 29 ...

INITIAL SURGE

While there had been bad weather looming on the radar, no one saw anything like the derecho coming. "The severity, the speed and the wind velocity that struck was quite unpredicted," Souder said.

911 centers throughout the region were immediately swamped with calls of downed wires and trees, felled poles, roof damage — all the typical carnage in the aftermath of intense wind and rain, but coming at an extraordinary pace.

During the three hours of the storm, 10:30 p.m. to 1:30 a.m., emergency call traffic in Fairfax County reached 415 percent above a normally busy Friday evening. Fire crews went out on rescue calls. Police took over manual traffic control at intersections where power outages had knocked out the signals.

There were early, though by no means catastrophic, blips in 911. When the Arlington emergency system lost power briefly, systems including 911 rolled to the uninterruptible power supply and then onto generators, as designed. Operationally, the power never went out. The generators ran for 10 hours until power was restored.

Emergency managers braced for the morning, when homeowners would wake up and realize the full extent of the damage to their properties. By 7 a.m., there would surely be a fresh wave of 911 calls.

Except there wasn't.

The new shift came on at 7 a.m. "And virtually at the same time we noticed that we were not getting any 911 calls — a most unusual thing — and we had not been notified by Verizon that there was any problem," Souder said. The emergency lines were out; the nonemergency lines were gone. The administrative and business lines: all dead.

"I got an email in the morning saying there were major problems, no 911 service at all, contact the department of public safety communications ASAP," Souder said. "I tried to contact them by my personal cellphone, but I found that even that was out."

He headed into work, where things were just as bad as he'd imagined. There were no telecommunications, period. "Obviously we have an alternative center that we would normally go to, but in this case it also was without any 911 service. This thing was as total as anyone knows of in the 44 years that 911 has been around."

911 went out at 6:30 a.m., and Fairfax managers didn't hear from Verizon until three hours later. Why the lag? It's far from clear. "Verizon has said their delay in notifying Fairfax County and other jurisdictions was because of technical problems and internal and external communications issues," Souder said.

In fact, the communications rift was even greater, Souder said. Verizon knew it had major problems on its hands well before 911 systems went down, but didn't reach out to local officials for nine hours. "I have described that as akin to the captain of the Titanic not telling his passengers the ship had struck an iceberg until the bow of the boat was about to hit the bottom of the ocean," Souder said.

"Obviously this was a situation that we had never encountered before. The only thing we could do was post a message on Twitter that, in fact, 911 service was out," he said. "We told people to go to the nearest police or fire station, to flag down the nearest police or fire unit and tell them of your emergency. It was not something we would ever want to do, but it was the only thing we could do."

The outage lasted in some places until July 3.

PICKING IT APART

Investigations are ongoing: Verizon is looking into its own systems; the FCC is sifting

VERIZON PROACTIVE IMPROVEMENTS

How can a 911 outage be prevented? In the wake of the northern Virginia events, Verizon has said it will make the following improvements:

ISSUES	CORRECTIVE ACTIONS
The systems suffered key generator failures that were different in each location. The specific failures have been repaired, but Verizon is extending its review of critical locations to address potential issues.	Conduct backup power system audits in mission-critical Verizon facilities supporting 911 in Virginia, Maryland and Washington, D.C. Institute any corrective measures identified in those power audits.
Verizon determined it could have improved restoration of service had it recognized more quickly the partial power outage in Fairfax and been able to power some network equipment (e.g., telemetry systems) on the one generator in Arlington that was working.	Develop and post site-specific backup power system assessment procedures to assess power loss to an area of a building. Develop and post site-specific manual generator start and transfer procedures. Enhance critical facility "blackout" testing.
Internal mobilization based on actual or potential service impacts should be triggered by alarms. The loss of visibility prevented managers from receiving these alarms and delayed the response.	Create two new event criteria for notification and mobilization purposes. Enhance notification and mobilization procedures to trigger activity faster when batteries are activated or when telemetry is lost.

Personal property was damaged throughout Fairfax County by fallen trees and other debris.

PHOTO COURTESY OF VIRGINIA DEPARTMENT OF TRANSPORTATION

FLICKR/FAIRFAXCOUNTY

Virginia Gov. Bob McDonnell, center, and Board Chairman Sharon Bulova held a news conference with media discussing the aftermath of the serious storms that struck the area on June 29.

through the ashes; the Virginia State Corporation Commission (the state regulatory body) is conducting its inquiry; and the governor's office and Metropolitan Washington Council of Governments are examining the outage.

Everyone wants to know why and how it happened, but at least the "what" seems clear.

A Verizon report from August put it succinctly: "External power failures affected more than 100 Verizon locations. At each of these locations, batteries and nearly all the back-up generators worked as designed, allowing us to continue service. However, at two of these locations, generators failed to start, disabling hundreds of network transport systems, and causing Verizon to lose much of its visibility into its network in the impacted area."

Two generators failed to fire up, and the entire 911 network in northern Virginia went down. The few emergency calls that did find a way through arrived without location information. The failed generators triggered a cascade effect that ultimately knocked out four public safety answering points. Compounding the problem, system failures included the downing of monitoring capabilities, making it impossible for Verizon to see into its northern Virginia network facilities, thus hindering initial efforts to assess and repair damages, Verizon reported.

A critical question remains: Why didn't the generators start?

Verizon conducted testing using third-party experts and found that in the Arlington facility, air had entered the fuel system, resulting in a lack of fuel in the lines. The fuel lines for both Arlington generators have been replaced.

Verizon found that the Fairfax generator did not power up because the auto-start mechanisms failed. Those mechanisms should start the generator once commercial power is lost. "But they did not operate correctly and have since been replaced," Verizon reported.

However, all this leaves Souder far from satisfied. The 911 system is used 240,000 times a day, 87 million times a year. "It is the gateway to public safety," he said. "It has to be flawless. It has to be robust. It has to stand up when it is most needed."

He's not the only one frustrated.

PROPOSED CHANGES

Discussing the derecho in a July 19 hearing, the FCC's Genachowski declared, "911 outages are unacceptable, and we must and will work with all stakeholders to address this serious issue."

The chairman sought to put a human face on the crisis. "In Prince William County, Va., someone called 911 to report a man suffering cardiac arrest and got a busy signal. He finally got help, fortunately, but only after the caller tracked down authorities on a nonemergency line. The derecho made clear the absolutely vital role of our communications networks, particularly during emergencies."

While various agencies investigate the outage, officials in northern Virginia already are making recommendations.

"Our feeling was that, while we still didn't know a lot, we did know some things that would make it a whole lot better, and we didn't want to wait six or eight months until the official reports came in," said Souder.

The 911 directors of Alexandria, and the counties of Arlington, Fairfax, Loudoun, Prince William and Stafford have recommended that Verizon adopt five steps that are primarily focused on communications in response to the storm. Verizon has agreed to all.

- Officials recommended that Verizon sign onto the National Incident

Next-Generation Emergency Notifications

Safe Towns

Keep your community safe and connected.

800-600-3911
INFO@AMERILERT.COM
WWW.AMERILERT.COM/SAFETOWNS

Amerilert Safe Towns™ is the most comprehensive suite of municipal safety communication services available. From one intuitive interface, it unites an award-winning emergency notification system, text-a-tip service, info hotline, crisis collaboration tool, and more. Get your free demo of this cloud-based, GIS-interfaced, CAP Compliant system today.

AMERILERT® gtsi® One Mission. Yours.

U.S. COMMUNITIES GOVERNMENT PURCHASING ALLIANCE

SAFE TOWNS AVAILABLE THROUGH GTSI VIA U.S. COMMUNITIES CONTRACT

EMERGENCY MANAGEMENT - DISASTER RECOVERY - CONTINUITY OF OPERATIONS - CRIME PREVENTION - MASS NOTIFICATION - COMMUNITY RESPONSE

Steve Souder, director of public safety communications for Fairfax County, says there have been lessons learned from using social media during the blackout.

Management System (NIMS) model to address future incidents. Verizon said it employs an "all-hazards approach" to its business continuity, disaster recovery, facility preparedness and emergency management programs. That process utilizes NIMS principles, and thresholds for invoking that process have been strengthened to more readily bring those procedures to bear in similar situations.

- It is recommended that Verizon obtain and use a reverse notification phone call system to give notice about an interruption of 911 service. Verizon notes that since March 2011, it has employed a broadcast email process to provide specific ticket information to individual public safety answering points. Verizon said it will expand that process to include texting and will work with 911 directors to establish the correct contact lists and process details.
- Emergency managers recommended that the company develop a semiannual drill or exercise with each jurisdiction on actions to be taken in the event of a 911 outage. Verizon said it will engage the assistance of its Business Continuity Emergency Management team to work with the company's 911 Customer Care Center organization to develop and exercise procedures for such drills.
- Verizon should provide, during the first week of each month, a current contact list for the account manager assigned to a given jurisdiction, along with contact information for four immediately escalating Verizon personnel up to a vice president level. The company agreed to do this.
- Verizon will have a representative present at the jurisdictions' EOCs to provide accurate information concerning 911 service and outages. Verizon said it will work with the 911 directors to explore ways to accommodate this request, perhaps through virtual participation in an EOC via an instant messaging-like application.

These initiatives won't guarantee that the events that occurred during the derecho will not repeat, but they should give emergency planners a solid start against future crises. "Not every one of these will apply in every location, but we know what we are looking for. So while the solution in each situation may be different, the overall plan will be comprehensive," said Maureen Davis, Verizon vice president of network technology for the Mid-Atlantic region.

Beyond these specific remedies, Verizon walks away with a greater appreciation for the overall vulnerabilities of its systems.

"We need to be more engaged with how social media can be utilized to notify the public," Souder said. "We didn't do a bad job, but we did it on the fly. It isn't something we normally do. We know the social media phenomenon has a role here, but how to use it, how to engage it — these are weighty things."

The 911 center doesn't have its own Twitter account. The communication after the derecho ran through the county government's account. Clearly, Souder said, something more formal is needed.

At the same time, local planners are assembling an intrajurisdictional 800 MHz talk group for 911 events, a network that would reach across the region's trunk radio systems without interfering with the police or fire mutual aid radio systems. "It will allow us one more communications path," said Souder.

LESSONS LEARNED

Was there an element of human error here? Not in the immediate sense: The breakdown was fundamentally mechanical. But there clearly were systemic difficulties, a failure to communicate down the line at crucial moments, and a shortfall in emergency procedures that might apply in the most extreme circumstances.

Could the situation happen again? Whatever flaws may have lurked inside those generators, it took an extraordinary meteorological event to bring them to light. History has shown that extreme weather can drive extreme consequences. It might not happen in exactly this way, but surely a catastrophic 911 failure can never be ruled out. What's more relevant is the response.

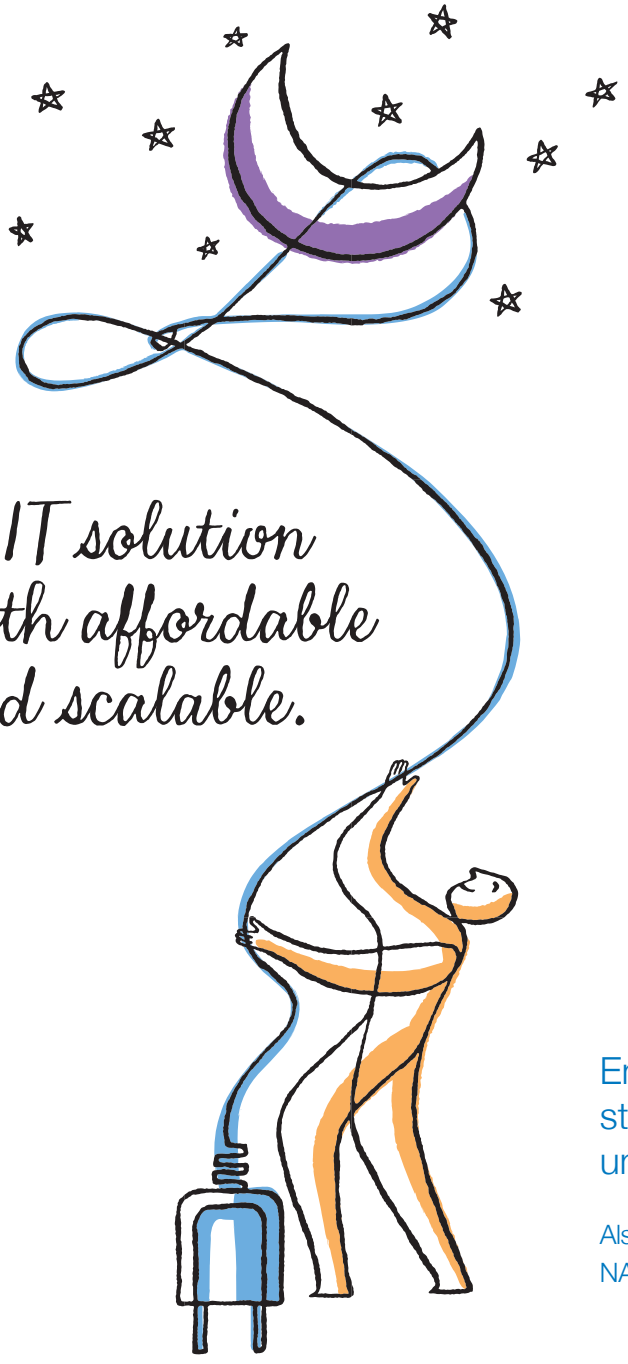
> "Obviously this was a situation that we had never encountered before. The only thing we could do was post a message on Twitter that in fact 911 service was out."

"For us, one of the major lessons has to do with ways to deal with significant and multiple catastrophic events," Davis said. "We have had commercial power failures and generator failures at central offices before, but I can't think of a single instance where we were working more than one at a single moment. We all just need to be continually vigilant about backup strategy, redundancy, diversity, so we understand how much of it we have and how much of it we need."

Emergency managers meanwhile found in these events a none-too-subtle reminder that their means of public outreach is still in need of upgrades.

Emergency managers have articulated a new set of safeguards that should help to drive response in future events. By the time investigators have finished combing through this crisis, they likely will have learned enough to stand up more robust defenses to aid during future disasters.

adam.stone@newsroom42.com



Choose an IT solution that's both affordable and scalable.

Enterprise-class storage starting under $8,000.

Also available on WSCA/ NASPO, B27170.

Smart decisions are built on **NetApp**®

To see how agencies with smaller IT budgets can finally choose storage solutions they won't outgrow, visit www.netapp.com/government.

Go further, faster®

Emerging technology could positively impact all phases of emergency management.

CUTTING EDGE

Albert Einstein once said: "The true sign of intelligence is not knowledge but imagination." Who can argue with that, especially when it comes to technology? Imagining how technology can fill a void is necessary when it comes to conceiving a new device or system. Perhaps nowhere is there an example of the importance of emerging technology as there is in emergency management. Thousands of people can be impacted by a man-made or natural disaster within seconds, and the availability of tools that can help not only before but also during the response to the devastation can save lives and time.

ELAINE PITTMAN | ASSOCIATE EDITOR

Emergency Management sought out emerging technologies that will positively impact the field and possibly change how people think tech fits into preparedness, response and recovery.

Within the last couple of years, social media has become go-to communication tools that the public uses to obtain information. But one of the issues for emergency managers is how an agency can test how it would use social media in an emergency. Tweeting and issuing updates on Facebook — even when preceded and followed by the words "test" or "drill" — would likely confuse people and possibly start rumors, which can be impossible to stop once the incorrect information starts to spread. But emergency management consulting firm Nusura Inc. is seeking to provide a way for agencies to test their social media and public outreach practices through the use of its training tool SimulationDeck.

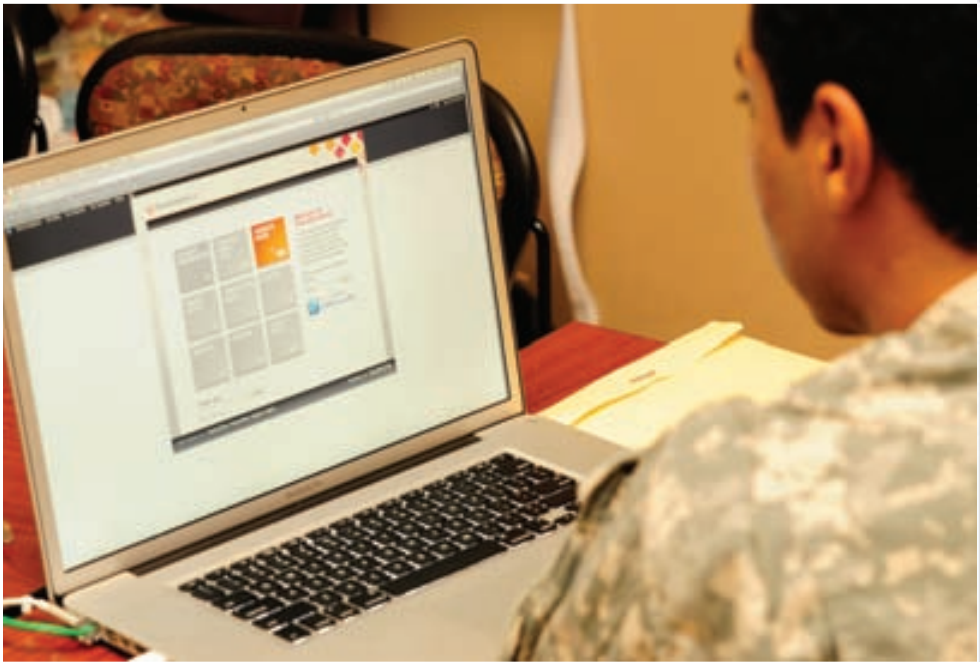
The secure Web portal replicates online communication tools, including popular social networking sites like Facebook and Twitter, as well as agency websites and blogs. Nusura President Jim Chesnutt is using his experiences from being a public information officer — including with FEMA as a deputy public affairs officer for Region VIII — to help people train on disseminating timely, accurate and coordinated public information during emergencies.

After participating in numerous exercises, Chesnutt observed a pattern: "In the after-action reports for almost every major exercise I worked on, they said that the public information function was not being tested in a realistic way. And it's true." The pressure created by mock media and those tasked with testing the public information element didn't compare to the reality of handling even a small emergency, he added.

Nusura — which is composed of former public information officers from all levels of government — created SimulationDeck to mimic what happens online and in the media during an emergency. The Web portal has nine websites: SimulationBook includes Facebook's core features; Bleater simulates Twitter; blogging platform Frogger; YouTube lookalike EweTube; agency news; incident information; Exercise Times Daily, a Web-based newspaper that features live reader comments; SimDeck News, a Web-based TV station; and KEXN Radio.

SimulationDeck doesn't require special software, so it can work on any platform or Internet-connected device. Chesnutt said one person working in the simulation cell during an exercise could act as 10 people. For example, he or she could file a newspaper article, then post on the agency's website and then act at the governor's press secretary and announce a surprise press conference. "Things happen instantly, and any simulation player can generate an enormous number of injects, as fast as they can type and hit enter," he said.

Although the tool hasn't been on the market for very long, it was used during Vibrant Response 13, a U.S. Army North national-level field training exercise that had about 9,000 service members and civilians from the military, as well as federal and state agencies. Don Manuszewski, chief of public affairs for U.S. Army North, said it's important to practice all forms of communication and that includes social media as it becomes increasingly popular. "Social media is becoming kind of a way that a large section of the population gets and sends out information, so if we're not training to understand how it affects us and where it's going, then we're doing a disservice to those we're trying to help," he said. "We need to make sure we understand the entire information environment from



SimulationDeck replicates popular social media platforms so public affairs officials and responders can practice using the communications tools during emergency exercises.

Panasonic
ideas for life

Connecting your city with cutting-edge technology is how we're engineering a better world.

SOLUTIONS FOR PUBLIC SECTOR

Panasonic
ideas for life

Enhance your city's communications and awareness, and protect citizens and property, with one company. Designed and built with unmatched reliability, Panasonic products give you the upper hand in first response and public safety with innovative solutions fit for any application.

FASTER RESPONSE TIMES AND HIGH-QUALITY VIDEO EVIDENCE

Fully-rugged Toughbook Mobile Computers

For emergency first responders, getting to the scene of a crime, fire, disaster or power outage is more than time critical—it's lifesaving. With industry-leading reliability, Panasonic Toughbook® fully-rugged mobile computers help improve response time and provide immediate, remote access to critical information en route to an emergency.

Toughbook 31 Toughbook 19

- IP65 and 6-foot drop certified for unrivaled ruggedness and drop-shock protection
- 3G or 4G mobile broadband and GPS-ready design allow immediate access to mission-critical information
- Adjustable sunlight viewable display and optional backlit keyboard keep first responders productive in any lighting condition

Mobile Digital Video Solutions

Law enforcement professionals need a reliable eyewitness backing them up. The Toughbook Arbitrator 360°™ and NEW Panasonic WV-TW310 Series rugged, wearable camera offer a digital recording solution that improves officer safety, reduces agency liability and maintains the integrity of the chain of evidence.

WV-TW310 Series and
Toughbook Arbitrator 360°

- The Toughbook Arbitrator 360° increases situational awareness by providing officers with a 360° view of their environment
- Wearable camera provides a wide-angle view with image stabilization and correction function on playback
- High-quality video resolution provides an accurate record of any situation

INFORM THE PUBLIC AT A MOMENT'S NOTICE

Digital Signage Solutions

State and local government play a key role in providing vital services to the community, making the immediate communication of the right message a necessity. With Panasonic's full range of digital signage solutions, government personnel have a system that quickly and easily communicates critical information to the public at a moment's notice.

From simple display installations to custom-designed multi-location networks, Panasonic combines world-class hardware with industry-leading software and media players, system build-out and management, and unmatched support to deliver a complete, reliable digital signage system tailored to your needs.

Panasonic's LF Series LCD displays maintain real-time communication with visitors and staff inside libraries, government offices, courthouses, town halls, community centers and other public buildings.

- Narrow 18mm bezel (0.72") for flexible installation vertically or horizontally
- High brightness IPS panels for clear messaging from virtually any angle
- Eco mode detects ambient light levels and controls brightness accordingly
- Fanless design for less maintenance

Display time-sensitive alerts, travel schedules, news and weather to the public outside buildings, airports or transit stations with Panasonic's LFP30 Series and LFT30 Series high-performance displays that can withstand the harshest conditions, including rain and dust.

- IP-rated weatherproof designs for outdoor messaging
- Up to 1500 cd/m2 brightness for excellent visibility outdoors
- Corrosion-resistant aluminum cabinet
- Winter Mode allows for operation in temperatures as low as -4 ˚F (-20 ˚C)

Panasonic
ideas for life

KEEP CITIZENS AND PUBLIC PROPERTY SAFE

Video Surveillance Solutions

Panasonic's surveillance video imaging technology increases situational awareness of events as they unfold, improves response time during emergencies and documents evidence that aids in the arrest, investigation and prosecution of criminals. With the finest end-to-end imaging in the industry, Panasonic provides a wide array of security solutions for your community.

For outdoor applications such as busy intersections, high-crime areas, airports, transit stations and waterways, Panasonic's WV-SW559 fixed dome camera is the ideal solution for video imaging. Designed to survive the harshest conditions, the WV-SW559 is weatherproof and can survive treatment shocks and impact. Equipped with Super Dynamic ABS and Face Super Dynamic range technologies, it covers a wider range than conventional cameras and enables a clear and precise image of a subject's face.

- IP66-rated and compatible with the IEC measurement standard for weather, shock, impact and vandal-resistance
- Full HD 1080p images up to 30 fps and multiple H.264 and JPEG streams ensure simultaneous, real-time monitoring and high-resolution recording
- Progressive scan ensures clear images with less motion blur and no tearing even when subject is moving
- Auto Back Focus allows for flexible installation and stable focus in both color and B/W modes

To monitor events in public buildings, Panasonic's WV-SF336 fixed dome network camera offers the highest standard of indoor security. With Wide Dynamic range, ABS and Face Super Dynamic range technologies, it enables clear and precise video recording and playback.

WV-SF336

WV-SW559

- 720p HD images up to 30fps with progressive scan and a 1.3 Megapixel MOS Sensor
- Multiple H.264 streams and JPG streams ensure simultaneous real-time monitoring and high-resolution recording
- Auto Back Focus allows for flexible installation and stable focus in both color and B/W modes

panasonic.com/business-solutions
GovernmentSolutions@us.panasonic.com

Intellistreets smart streetlight poles could detect rising floodwaters and even display the evacuation route to help citizens and visitors safely leave an area.

the traditional media to the media that people are using now like social media."

U.S. Army North incorporated social media into previous exercises to varying levels of success. For example, U.S. Army North used milBook, a professional networking site similar to Facebook that was developed by the U.S. Defense Department, during training but it didn't quite work because the organization was trying to adapt it to meet its needs, instead of vice versa.

Using SimulationDeck during Vibrant Response 13 felt more real than previous attempts at incorporating social media during an exercise, Manuszewski said. "It met our needs much better than anything that we have used in the past." After the exercise, they worked with Nusura on some features that could improve it. For example, Manuszewski said people on the microblogging site couldn't track a trending topic. The workaround was to create a page and name it with the topic that staff wanted to track in place of being able to utilize a search feature.

Nusura's Chesnutt said updates have been made based on user feedback and SimulationDeck also evolves to reflect real-world changes. "It is organic and ever changing just like the Internet," he said.

INTELLISTREETS

Intellistreets' smart streetlight poles connect to a Web-based system so officials can remotely update the attached LED signs with important information like an evacuation route.

What if lampposts could detect rising floodwaters and even display the evacuation route to help citizens and visitors safely leave an area? That is what Ron Harwood is trying to do with Intellistreets, an emerging technology that outfits streetlight poles with wireless technology to provide emergency alerting, homeland security and public safety functions as well as energy conservation.

"The system was invented as a response to the chaos created at street level during 9/11," said Harwood, president of Intellistreets. The company can retrofit existing streetlights if a community isn't ready to purchase brand-new, high-tech poles, and while the features vary depending on an area's needs, they can include: emergency alerts, digital signage, hazardous environment alerts, two-way audio, vehicle impact detection and a pedestrian counter.

At its heart, the technology consists of a dual radio mesh wireless system that has embedded microprocessors, which Harwood said allow for information gathering, such as analysis of what a streetlight is hearing, seeing, smelling, etc., a method known as edge processing. "The advantage is that first responders get real information interpreted into English or graphics that comes right from the site instead of analytics that happen through backhaul technology and processors," he said.

Accessed via a Web-based system, operators and first responders can receive an alert when an environmental factor triggers the system. Because the technology is built into each streetlight, the government representative can take action from a remote location to make pedestrians aware of a situation. Harwood gave the example of outfitting streetlight poles with water sensors. In an area that has flooding or water main issues, a streetlight with the built-in intelligence would activate a warning light when water reaches a certain depth like being detected above the curb. Other streetlights in the area that have the technology would begin to flash, warning traffic to slow down.

Intellistreets' audio features also increase public safety in a two-way fashion. Emergency blue light buttons allow people to signal for help, and speakers provide a way for government officials to make announcements or issue emergency alerts. Digital signs can display standard information, such as civic announcements, and then be updated with crucial information like an evacuation route when necessary. The system features built-in signage and announcements for standard situations that allow a public safety representative to click a button on the Web-based system to start audio alerts or change what's being featured on the digital signs. Harwood's goal is to have an iPad in each patrol vehicle so officers can easily update the messaging when needed.

The technology is not widespread yet, but is being used at Sony Pictures in Culver City, Calif., where the digital signs provide departure routes during the movie lot's weekly evacuation exercise.

We take the worry out of NextGen 9-1-1.™

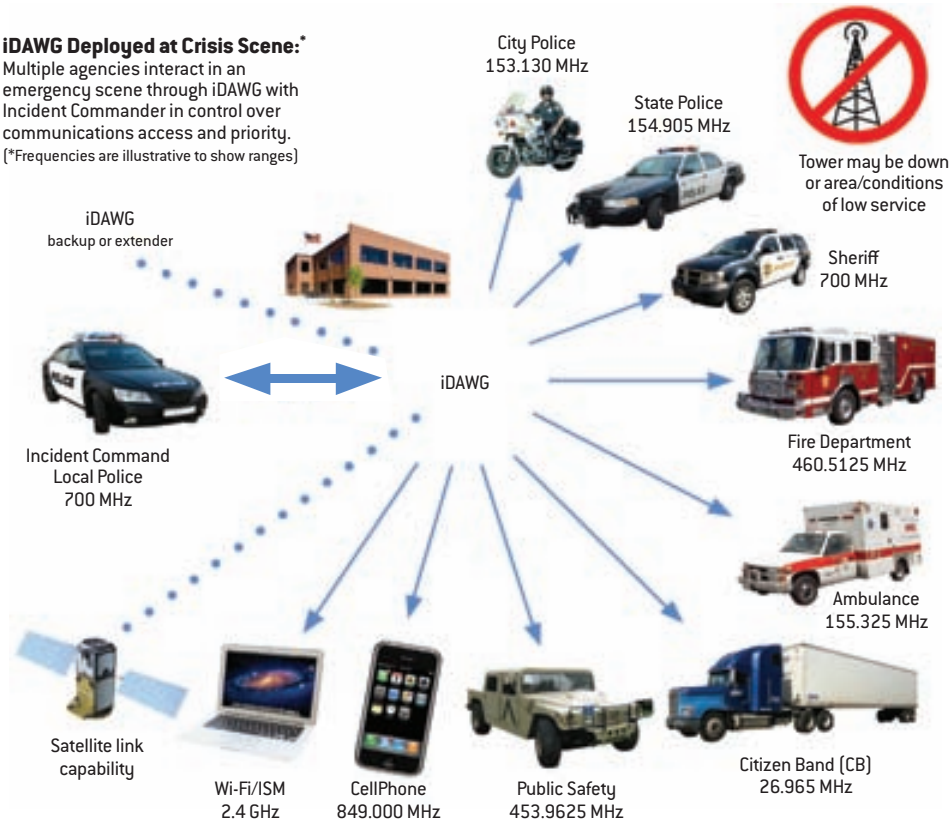
Intrado has the reliable, proven path to next-generation 9-1-1. With the Intrado Great Migration, you get a fully managed package of Advanced 9-1-1™ solutions with no capital outlay, guaranteed i3 compliance, and predictable pricing. It's the safe, smart way to make the move to NextGen 9-1-1.

Learn more at **www.intrado.com/greatmigration**

intrado®

Additionally, a demonstration of Intellistreets was installed in Farmington Hills, Mich., last year. Although the local government isn't using the system's high-tech tools, its officials think the features would be beneficial. "I think the potential for them is huge," said City Manager Steve Brock. "We haven't used much of the technology that I think is available with regard to messaging, signage and things like that. But when we went through the demonstration of them, when they sort of christened them, if you will, I was very impressed with their capabilities and what it could mean in all sorts of environments."

During a worst-case emergency scenario, communication between responders is both necessary and difficult. Much research and effort has gone into interoperable communications, including at Syracuse University's School of Information Studies where a device is being developed that will maintain commu-



nication between different devices without relying on cell towers or Internet networks.

The iDAWG — Intelligent Deployable Augmented Wireless Gateway — works with a new class of software, called edgeware, that connects devices and information and helps with machine-to-machine communication. Professor Lee McKnight said the process is similar to ad-hoc networking in which a local network is built spontaneously as devices connect to one another. McKnight explained that when a user connects to a wireless network during everyday life, he or she doesn't connect computer to computer because of increased security risks. Following a disaster, however, it could be one way of communicating and connecting with others. According to a university paper, iDAWG is an "infrastructureless wireless network based on a cognitive radio-based field deployable unit with information sharing/communication capabilities."

The paper stated that: "The iDAWG is designed to securely capture and share multiple wireless transmission media including police, fire, EMS, municipal, private, cellular and CB bands by acting as a signal repeater to provide or extend service on scene."

Joe Treglia, assistant director of the university's Wireless Grid Innovation Testbed, said technologies for interoperability in data and communications like iDAWG and edgeware are significant for communication between traditional and nontraditional responders during an emergency.

The School of Information Studies' students and professors are working with public safety and emergency management representatives to understand their needs. They observed a multiagency exercise in August and have demonstrated some of iDAWG's capabilities to a local 911 call center and an immigrant relocation group.

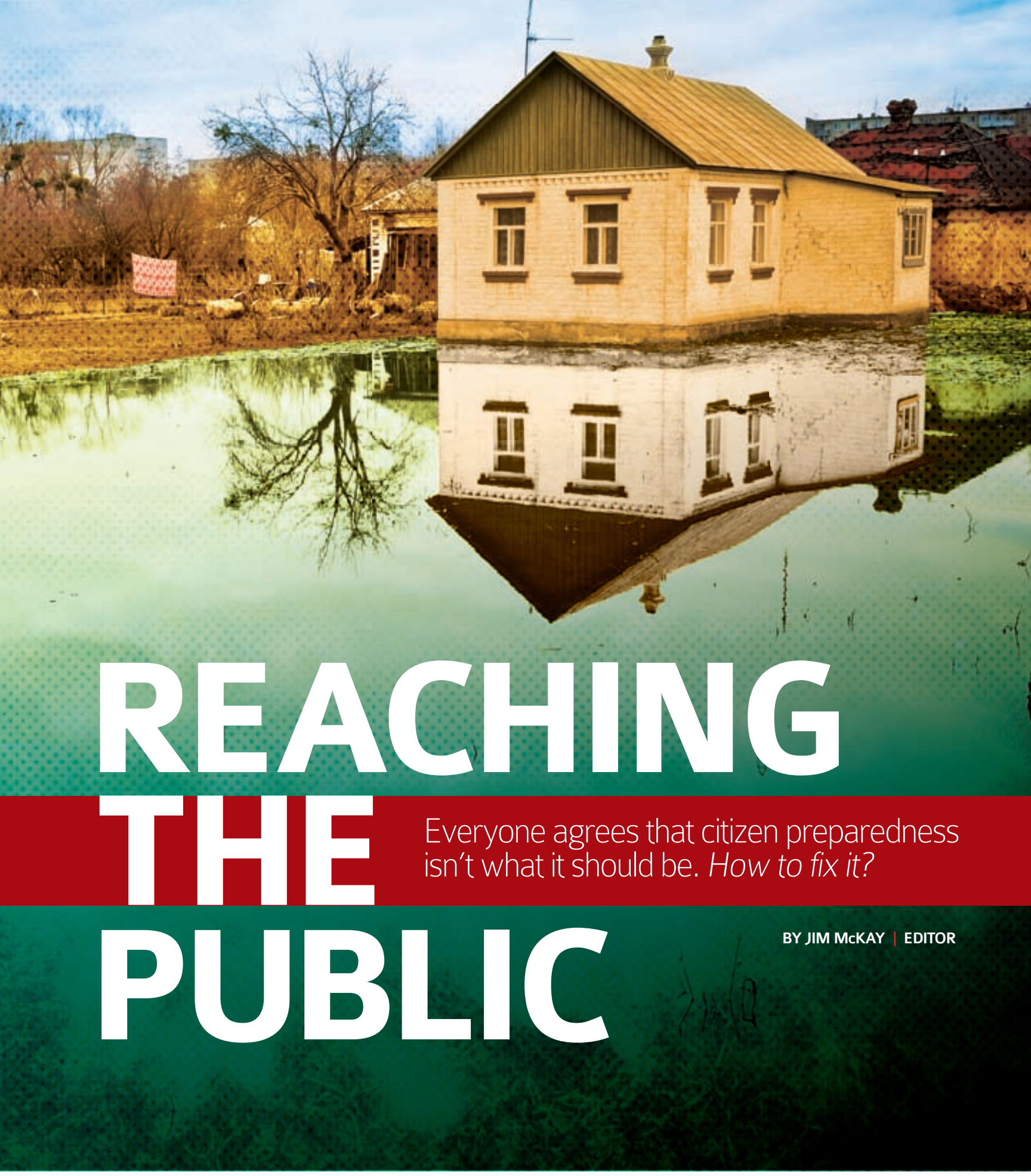
"The involvement of university researchers with practitioners and the public is a fairly new collaborative arrangement that brings new broader insights to the issues and creates actual solutions for incorporating this new way of operating and managing crises," Treglia said.

In addition to iDAWG's core components, Syracuse University researchers are working with the Rochester Institute of Technology's low-flying plane that captured imagery of the destruction from real-world events like the magnitude 7.0 earthquake that struck Haiti in January 2010. Developed by the Information Products Lab for Emergency Response, the plane could continue to deliver the images to incident commanders through iDAWG even in the event that cell towers and the Internet are down. "The iDAWG is designed to be capable of receiving and then relaying these kinds of emergency field images," McKnight said.

The iDAWG is also going to be able to work with FEMA's Integrated Public Alerts and Warning System. The research is receiving funding from the National Science Foundation Partnerships for Innovation Program and includes Virginia Tech, Syracuse University and the Rochester Institute of Technology.

epittman@emergencymgmt.com

TOM McKEITH



REACHING THE PUBLIC

Everyone agrees that citizen preparedness isn't what it should be. *How to fix it?*

BY JIM McKAY | EDITOR

Americans have a false sense of security when it comes to disasters, and should they become victims, most haven't taken steps to help themselves during the first few days after one strikes. Experts say either the preparedness message isn't getting across, or the wrong message is being sent.

In a recent survey conducted by the Ad Council, 17 percent of respondents said they were very prepared for an emergency situation, which means they have a kit and a plan to sustain themselves during the first few days of a disaster. In the same survey, however, just 23 percent of respondents said they have a plan to communicate with family members if there is no cellphone service.

But this figure is considered inflated by some who say the percentage of prepared citizens is dreadful. "Oftentimes you'll get a survey saying 6 percent of the public is prepared," said Ana-Marie Jones, executive director of the nonprofit organization Collaborating Agencies Responding to Disasters (CARD). "That's nothing to write home about if you consider 4 percent of the population is Mormon and they prepare without being told to do so by the U.S. government."

Jones said the methods for reaching the public leave a lot to be desired. "No private company would invest billions of dollars putting a message out that had such dismal returns," she said. "You just would never do it."

Jones took part in an event this summer, called Awareness to Action: A Workshop on Motivating the Public to Prepare, hosted by FEMA and the American Red Cross. The two-day event invited 85 preparedness experts from across the country to discuss how to engage the public with preparedness. Jones said the majority of attendees agreed that the message is flawed.

"The highlight of the two days was [FEMA Administrator] Craig Fugate coming to the meeting and being honest in saying we have to acknowledge that we haven't moved the preparedness needle," Jones said. "When the highest person in FEMA acknowledges that it has not been a success, it gives me hope."

A Negative Message

The message is to have a kit, be aware of potential emergencies and have a family plan. The problem is that it's generally based on fear, according to some emergency management professionals. But to some, being prepared takes a backseat because they've never experienced a catastrophe.

"A mind-alerting event has not taken place in their lives to drive them to take some preparedness actions," said Will Allen, retired colonel and CEO of consulting firm W. Allen Enterprises. He said most people don't see preparedness as an important issue because of how it's presented. "It has a lot to do with people's experiences, their culture and awareness. Maybe our local government hasn't made it an important issue to them."

This dog lives in a coastal area in California and a pet life jacket was included in her owner's emergency supply kit. *Photo by Carolyn Deming*

Jones said the "have-a-kit, be aware" message is OK, but the way it's conveyed is problematic. "It's threat-based, top down, put forth by agencies whose mission, mindset and muscles are around disaster response, not preparedness," she said. "There's a different way to leverage resources in a community than to tell everybody, 'You need to have this, otherwise horrible stuff is going to happen to you.'"

The message is more like a "branding campaign" for the agencies, Jones said, and tying preparedness to specific threats like earthquakes, hurricanes, floods and terrorism is telling 90 percent of the population not to worry. "There's a ton of research that shows that threat-based messaging and showing the horrible pictures of the collapsed buildings and the floating dead bodies does not help you prepare, but stops you from preparing because it triggers the overwhelm factor."

The proper message isn't tied to having a kit but to developing resilience every day.

The consensus is that many families don't have an emergency kit. "We say, 'You need to get a kit that has food, water, a radio, flashlight.' The list goes on and on," said Dallas Emergency Management Director Kevin Oden. "Well, those costs really add up and most people can't do that." He said it's better to ask people to prepare over time by bringing home extra water or nonperishable food when possible. And the best kits are not ones that were purchased whole but the ones built from supplies families use regularly and will use during a crisis.

Even that is difficult for those who struggle daily to take care of their basic needs. "If I didn't eat this morning, that's real," Allen said. "I'm supposed to be prepared for something that may or may not happen? I haven't even thought that far ahead. It's going to require a different effort."

Allen said getting people to purchase items they might need in an emergency will take incentives. "I need to eat; I need shoes, so come at me with some way I can get that, such as a Target coupon. Something like that would be a lot less costly than some of the actions we have to take after an event."

Jones agreed, saying citizens will prioritize what's valuable to them right now. "That's

always the way it will be. You're never going to get people to prioritize the earthquake, flood or act of terrorism over their daily needs."

Jones stressed that citizens are much likelier to develop resilience by focusing on things that could help during a disaster and every day, like a cellphone.

"If I told you to put aside your computer until you need it for a disaster, by the time you needed it you wouldn't be familiar with it," Jones said. "That's exactly what happens with our disaster stuff. You'd have a better shot with a cellphone."

She said people should program the names and phone numbers of their neighbors, employees and relatives into their cellphones. "If you don't have resources like food and kits, maybe somebody else does," Jones said. "Maybe you've got other resources. Maybe you're the guy with the power tools or the big backyard where everybody can meet."

Oden said it's important for citizens not to think of disaster preparedness as a one-time deal. "If you're building preparedness over a long period, it's in your head and you're more likely to take additional steps to be prepared than if you bought a kit and put it in a closet."

Jones and Allen echoed that sentiment. "Anything that you can build into your everyday muscle is much more likely to serve you in a crisis," Jones said.

"Resilience is about getting better over time," Allen added.

Community Affiliations

Emergency managers shouldn't pass up an opportunity to educate residents on becoming prepared, however they shouldn't expect dramatic results. Local community groups that residents identify with and trust are best to push out the preparedness messages.

Community organizations, churches, schools, businesses and the like are better positioned in the community to deliver a more resonating message.

"People need to hear the message from people they believe in," said Jones. "If you want people who are affiliated with religious groups to get the message, they'll get the message when that religious organization threads it into a way they speak."

In addition, community groups are the only way to reach certain segments of society, such as non-English speaking residents who may not trust government. That will become

Ana-Marie Jones, executive director, Collaborating Agencies Responding to Disasters. *Photo by Jessica Mulholland*

A **FEMA employee** displays an emergency kit while conducting a FEMA For Kids Workshop. *Photo by Hans Pennink/FEMA*

more significant in the next 15 to 20 years as the Hispanic and Asian-American population is estimated to grow by 18 percent, Oden said.

"If we as government can't either linguistically or culturally connect to groups of people, a level of trust is hard to get," he said. "Take for instance our outdoor warning sirens that we use for severe weather. People who are non-English speaking are going to have a harder time getting the message of what warning sirens really mean to them."

Citizens tend to be somewhat *passé* toward government warnings, as evidenced by some of the response to a Federal Signal survey, which suggested that most people need to be able to validate a warning from another source. In the survey, 23 percent said they'd need to hear about local property damage before they became concerned. "The sense that bad things happen to other people is a real concern," said John Von Thaden, general manager for alerting and notification systems at Federal Signal.

That's where community groups can help. Von Thaden said there are big differences in the way some emergency managers coordinate with local organizations and communities, but it's important for emergency managers to do it. "It's a piece that emergency managers are looking for," he said. "It continues to grow as a role they play."

Allen used the military as an example of an organization having a captive audience. He said that when top brass wanted something known, they presented it to a controlled audience in multiple ways.

FEMA Administrator **Craig Fugate, left,** recently met with experts from around the country to discuss preparedness. *Photo by Karen Nutini/FEMA*

There are a couple of lessons there, and one is that people listen to and heed a message from organizations that have their direct attention. People need messages in different forms, and they need it from trusted sources, like churches, schools and employers.

"What you should do is seek out groups and community leaders, be it community centers or churches," Oden said. "People are much more connected today to groups of like interests than ever before, and if we as emergency managers are focusing on the leaders of those groups, then they can pass the preparedness message down to citizens."

Another approach is to penetrate schools. Jones said schools could start teaching about disaster preparedness as early as preschool. Two- to 3-year-olds can learn to crawl to a safe spot and know by color codes which areas are safe. A green-colored carpet under a table could signify safety, and kids would learn to be safe, not scared.

Social media also is a tool for communities to use for preparedness. "Facebook is way more resilient than most local governments," Jones said. "I'm located in Oakland, Calif., and I can promise you after the next catastrophic earthquake, Facebook will be more resilient than my city. It's little things like that spread across a community, more than it is big government-mandated interventions that work."

Diverse Approach

There are commonalities between the gaps in both preparedness and the public's response to alerts, as evidenced by the previously cited Federal Signal study statistics. "I think it speaks to the fact that many Americans have been complacent," Von Thaden said. Just as telling everyone to buy a kit is ineffective, using one message or method for alerting is ignoring portions of the population.

The key to reaching different population segments is to diversify the methods for alert notifications because preferences for alerts vary greatly among individuals. "Often it can be age or regionally related in terms of their experiences, and that can be anything from looking for text messages, a phone call or traditional messaging through radio and television," Von Thaden said.

He said a layered approach to notification is necessary and includes a mode for residents to validate the initial warning. Part of the hesitation of citizens is a disconnection with local emergency management strategies. For example, 71 percent of respondents in the Federal Signal survey didn't know if their community had a personal alerting and notification solution.

Von Thaden reiterated that emergency managers who partner with local community organizations do better in terms of having the public's ear.

He said putting the decision of how to receive alerts in the hands of the recipients by offering multiple options is important. It's a form of empowerment that a successful preparedness program should include.

"If we're building a system of empowerment, we're building preparedness," Oden said. "Anytime someone feels empowered, they are always going to be more likely to pursue something. It's just human nature."

jmckay@emergencymgmt.com

CENTER FOR DIGITAL GOVERNMENT

Issue Brief

New Era in First Responder Training

Collaboration Solutions Bring Dynamic Possibilities

The End of Business as Usual

The number and types of challenges faced by fire, police and emergency management organizations are expanding and evolving faster than ever before. We're also seeing a convergence of threats — from domestic disturbances and terrorism to natural disasters. That presents new dangers, and demands new tactics, techniques and information if our people are to work safely and effectively.

Training of first responders needs to go beyond classroom lectures and textbook memorization. It needs to impart skills and competencies for handling the demands of the job in the real world. Short of conducting training sessions inside a burning building or in the immediate aftermath of a crime or disaster, the closest we can get to an authentic training experience is through the use of multimedia materials. Imagine the impact of video footage of actual fires, arrests and other real-life situations in a training class. Consider the possibilities of real-time communication between instructors and students in different locations. Anything that brings the urgency and grit of a scenario to life will help better prepare the student for the real thing.

Furthermore, new recruits are energized by the way digital cameras, tablets and social media continue to transform our lives. They expect all of life to be similarly engaging — training included. We've even seen some first-responder recruits who have recorded training sessions with their own digital cameras so they can share them later with their colleagues via social media. These new students engage, and want to engage, with content in a whole new way. We need to be aware of the new tools out there that will help us meet them where they are.

As leaders, we also need tools to help us allocate our scarce human resources while documenting, optimizing

Quality training for first responders is essential.

ISTOCKPHOTO.COM

"We want firefighters to get immersed in their roles. We want them to feel like they're really on an emergency scene. In real emergencies, there's no interacting with a computer, there's no keyboard, there's no sitting down, there's no mouse."

- Bill Godfrey, Deputy Chief of Training and IT, Orange County, Florida, Fire Rescue Department

and streamlining training activities across the whole enterprise. It isn't enough to simply require training for a certain number of hours. We can't split our teams up and train half at a time, especially if we want to improve unit cohesion. Neither can we afford to backfill resources when we pull them off their duty stations for a class. We need new ways to reduce the logistical hassles of training and reach an entire team at once — without pulling essential resources off the street.

The cumulative result of these trends is simple: *Powerful and effective training for first responders is more important than ever.* More specifically, we need to train more first responders faster while increasing engagement and retention.

ISTOCKPHOTO.COM

Time for a Serious Upgrade

The days of the in-person classroom and the traditional dry erase boards are over. In today's training, the technology has received a serious upgrade. In fact, leading jurisdictions like the Essex Police in the U.K., the Searcy County, Arkansas, Fire Department in the U.S. and the Canadian Red Cross are charting a bold new path forward.

"You need to make training sessions relevant to the work that officers are going to be doing, but if you can relate the training room scenario to something more practical, and get officers more involved in the training, then you know they will learn more from the course. That's one of the areas where the [collaboration solutions] have really helped."

- Sgt. Andy Spink, Trainer, Essex Police, U.K.

These pioneers are leveraging collaboration solutions to reinvent training. Collaboration solutions include intuitive interactive displays — connected to computers — collaboration software and remote-connectivity products. They are much more than a place to capture diagrams or draw pictures. Users can write over content in digital ink and fully interact with both online and offline content — making it easy to share content and capture ideas in powerful ways. With or without an Internet connection, collaboration solutions allow for media-rich interaction and engaging content. Instructors can connect users to follow-up resources that they can take with them or access outside the classroom.

Multimedia training is the next best thing to live exercises. It provides an authentic training experience by incorporating video footage of real-life situations. A collaboration solution allows instructors and participants to annotate and interact directly with the video for a more engaging and productive experience. Participants can use video of an arrest to learn the proper procedures for apprehending a suspect. They can see video from a fire scene to learn how to collect evidence. Or they can simulate a hazardous materials disaster to learn new safety skills and response capabilities. The possibilities are unlimited, especially when multiple jurisdictions share training content with each other.

This kind of interaction changes instruction from a one-way transmission from teacher to students into a two-way learning environment where students interact with the instructor and the content. We also get a learning environment that is more engaging and more effective at ensuring that the concepts and techniques go beyond "book learning" and are understood at a deeper level.

Collaboration solutions offer the capability for **remote participation** — even if you can't get the whole team to one location for a training session, everyone can still share and experience the training via interactive display (collaboration solution). Teams that work together can now train together, even if some can't be there physically in person. This won't just cut costs and raise efficiency; it will also ensure that everyone is getting the same training on the same material. Allowing remote participation means, for example, that you don't have to pull firefighters out of the station for training sessions. We can bring the training to them, ensuring that someone will always be there to cover their districts — essentially "boots in the street" all the time. This can really reduce the logistical complexity of training your people.

A collaboration solution enables a whole new range of ways to **engage with the content** — regardless of one's physical location — by connection through a laptop, tablet or another interactive whiteboard in a different location.

As leaders accountable for training in our organizations, we need to ensure that **consistent training standards** are enforced in the process across the organization. We need visibility into who is being trained and when. We must ensure that quality instructors and content are being delivered across a multitude of settings. We need tools that will help us handle a bigger, faster paced and more rapidly changing job than ever before. Collaboration solutions provide these benefits.

Proving the Model Around the Globe

A number of jurisdictions have already developed and implemented this new high-tech approach to making their people ready for everything that might be thrown at them. The **Essex Police** operate in an area that borders the counties of Suffolk, Cambridgeshire, Hertfordshire and Kent along with four boroughs of the City of London. The Essex PD is responsible for two seaports, two airports, five urban towns, a number of small villages and some major thoroughfares. It manages the full spectrum of challenges that any modern police department faces in any part of the globe.

The Essex Police also know that their officers want to be out doing their jobs, not sitting in a classroom taking notes. Essex wants to engage its officers so they are prepared when they need to handle a call. With proper training, the Essex officers acquire all the information, skills and capabilities they need before those skills are called upon.

The Essex Police turned to collaboration solutions to get the job done. Essex Police Sgt. Andy Spink describes the approach this way: "You need to make training sessions relevant to the work that officers are going to be doing, but if you can relate the training room scenario to something more practical, and get officers more involved in the training, then you know they will learn more from the course. That's one of the areas where the [collaboration solution] has really helped."[1]

The same can be said of Arkansas' **Searcy Fire Department.** Trainees there need to build real skills and capabilities, not just spend time listening to lectures. That means seeing and feeling how they would react in a real situation when they're literally under fire. The Searcy Fire Department found that a collaboration solution has transformed their training.

"[The] interactive whiteboard [collaboration solution] has changed the way firefighters train, enabling them to test their skills fighting a virtual fire in a controlled classroom environment," says Doug Baker, training officer at the Searcy Fire Department. "It is easy to use, makes our training interactive and more interesting and challenges the firefighters as they test their skills with fire scenarios in and around Searcy. It teaches them to think through the firefighting process and to be aware of possible dangers such as a building collapse or an explosion."[2]

Collaboration in Emergency Response: Benefits Outside the Training Room

Collaboration solutions have major value in improving the training environment — but they don't have to be pushed back into the corner when training is finished. They can become an ongoing resource for better meetings, collaboration and even for handling real-time incident response. In fact, collaboration solutions are increasingly becoming the core of communications in live incident response situations and day-to-day operations.

CANADIAN RED CROSS/FLICKR

The Canadian Red Cross is a great example. According to Operations Manager Golnaz Aliyarzadeh, "The interactive whiteboard [collaboration solution] has improved the efficiency of our office. It's not only easy to use — it's more environmentally friendly because we use less paper. ... Rather than printing meeting agendas, we now use the board."

Getting Your Team Started

If you like what you hear, ask yourself: How can you move and transition your organization from the way it learns now to this new way of thinking? No topic is more important to a top leader in an organization than how to develop, retain and promote your employees' skills. Top leaders, then, need to make this a priority and to define the problem by answering the following questions:

- How effective are your existing training methods?
- How well does your force retain training knowledge and skills?
- Is it important to train your workforce faster AND more efficiently?
- Who do you need to train?
- Where are they physically located?
- What are the costs and challenges of getting them into a physical training room?
- How much training is one-time, and how much is ongoing?
- Would the integration of video, Internet access, and interacting with digital content improve the training environment?
- What's the value of greater engagement in your organization?

Once you've assessed your situation, educate the organization about what's possible. Reach out to vendors of collaboration solutions for case studies and information. Study the success stories, and contact some of these other jurisdictions to understand what they've done in their own work. This will help you choose your own strategy for moving forward. You will find that after reviewing your current training curriculum, and considering how to make those topics and your training schedule more engaging, you will end up with a plan that you know will better prepare your people to respond to the challenges faced in the field. You'll reduce the number of classroom days and be able to get your people back into the field more quickly and cost-effectively than ever before.

To summarize:

1) Gather support within the organization for the proposed change in approach.
2) Pilot-test collaboration solutions in a limited setting to understand how they are different from the way your team trains today.
3) Assess the return on investment from the pilot tests: What were the results and might they enable you to cut costs and train more effectively?
4) Proceed to a full rollout of the transformed organizational model.

At the end of the day, it's all about the safety and effectiveness of our first responders. Making sure they are there for our constituents, and for their own families, involves more than what happens on the day of any given operation — it depends on training. In the words of Bill Godfrey, deputy chief of Training and Information Technology, Orange County Fire Rescue Department in Florida, "We want firefighters to get immersed in their roles. We want them to feel like they're really on an emergency scene. In real emergencies, there's no interacting with a computer, there's no keyboard, there's no sitting down, there's no mouse. The only way to get that kind of realism is with the interactive whiteboard [collaboration solution]."[3]

For more information on first responder training solutions, visit http://info.smarttech.com/firstresponders.html.

Endnotes

1. "Essex Police: Interactive technology brings efficiency and relevance to police training," SMART Technologies Case Study, 2008.
2. "Searcy Fire Department: Technology transforms the way firefighters train," SMART Technologies Case Study, 2011.
3. "Orange County Fire Rescue Department: Making emergency response training safe yet realistic," SMART Technologies Case Study, 2011.

SMART™

SMART Technologies is a leading provider of collaboration solutions that change the way the world works and learns. As the global leader in interactive whiteboards, our products have transformed teaching and learning in more than two million classrooms worldwide, reaching over 40 million students and their teachers. In business, our Freestorm visual collaboration solutions improve the way that people work and collaborate, enabling them to be more productive and reduce costs.


EMERGENCY MANAGEMENT
NAVIGATOR
Free two week trial
at centerdigitalgov.com/emnavigator
What Solutions are Emergency Leaders Looking to Buy Now?
Inform Your Sales Team with our NEW Precision Online Tool.
✓ RFPs and bids in public safety and homeland security
✓ Contacts and funding data for UASI Regions
✓ Contacts for Fusion Centers
✓ Contacts and procurement data for the top public safety & emergency management jurisdictions
✓ Major grants and funding streams
✓ And Much More!
Powered by the CENTER FOR DIGITAL GOVERNMENT

On Message

Ana-Marie Jones is the executive director of Collaborating Agencies Responding to Disasters (CARD), a nonprofit in Oakland, Calif. CARD was created after the 1989 Loma Prieta earthquake by local agencies to train nonprofits and faith-based agencies in disaster preparedness.

Jones attended a recent two-day event, Awareness to Action: A Workshop on Motivating the Public to Prepare, hosted by FEMA and the American Red Cross to discuss emergency preparedness messaging to citizens. We asked Jones about the workshop and preparedness in general during a recent interview.

By Jim McKay | Editor

JESSICA MULHOLLAND

What was your impression of the FEMA/Red Cross workshop?

In theory, it was supposed to be 85 preparedness experts across the country convened by FEMA and the Red Cross, and the topic was about messaging — in particular: Get a kit, have a plan, be informed.

I have long been a proponent of how ineffective that message is and I thought that those individual pieces aren't grand. I mean, really, it's great to have a plan put together and a kit — the concept is perfectly fine. It is that it has been a dismal failure as a rally cry for the public.

What's wrong with the message?

It's threat-based, top down, put forth by agencies whose mission, mindset and muscles are around disaster response, not preparedness.

By anchoring preparedness specifically to earthquakes, floods, terrorism and other things we can't control, we've absolutely told 90 percent of the public, "Don't worry your pretty little head about this."

We spend much more money branding the emergency management agencies than we do preparing the public. If you look at the campaigns that are put out there, they aren't preparedness campaigns, they're branding campaigns.

But if you're going to give a big, broad-based, scattergun preparedness message, it should be nonthreatening and something everybody can do.

It's such an upper-class, American-privileged message to think that people have resources for sometime in the next 30 years when there's an earthquake.

Which is why we go so heavily on everyday brilliance being your disaster resilience. I can go into a homeless center and [teach] people preparedness skills that help them right now. People are totally willing to learn it, because it's of value right now. If I go in and give them whistles and teach them the emergency code (instead of a brochure) — one is yes, two is no, three is help — people immediately embrace this. Why? Because they feel a level of threat every day.

If you're a homeless person and you've got kids in that homeless center, I can tell you it's a moving experience for them because finally they get to be the good parent who showed their kid a tangible skill so that the kid can feel safe.

If you're a parent and living in a homeless shelter, you have that constant shame of having brought your kid into homelessness and you are constantly worried that somebody is going to fall off their meds, go off program, mess with their kids, molest their kids, you name it.

So that little whistle becomes this incredibly valuable thing. I promise you, nobody has responded that way to a brochure. And it will never happen.

What's the right way to get the message across?

The message that we at CARD have embraced is all about being prepared to prosper. Have your everyday brilliance be your disaster resilience. Anything that you can build into your everyday muscle is much likelier to serve you in a crisis.

There are lots of ways you can have your everyday brilliance be your disaster resilience.

It's never going to come by threatening the public.

In fact, CARD's website put up the study that the Red Cross did in 1992 and it was a brilliantly done bit of research. The organization went to the community, did basic disaster education for earthquake, fire and flood. They did two different classes. One class was given the preparedness message with disaster images; the other was given the same thing with no images. The results? Those who had the images did much less, and in some cases, nothing.

We're doing a lot of things that fall into the category of unintentional harm. Threat-based campaigns don't work.

You give people a threat-based message, they have to buy into all of the bad things. Terrorism is the best example. Look at how hard the terrorism message is for people to embrace. It's even harder than the national disasters.

We think there's a different path.

Talk about what a viable message should contain.

We have several initiatives that are all about getting people connected. We have one initiative that's nothing but cellphone. Become a freak about your cellphone.

Get your neighborhood in there, get all your emergency numbers in there, get your ICE [in case of emergency] contact in and label the people who are your neighbors so that your phone is your brilliant portable document storage.

The thing is whether or not you ever have a disaster and you need to crack into the kit, the communications stuff will help you for anything. There are a hundred good reasons to have your neighbors programmed into your phone.

There's a different way to leverage resources in a community than to just tell everybody you need to have this, otherwise horrible stuff is going to happen.

Ana-Marie Jones shows a portable folder that contains preparedness training materials.

JESSICA MULHOLLAND

Should emergency managers be charged with the preparedness message?

Technically, you would say it is their job, but they're not the right people to be putting forth that message. I believe, and this is where the public can play the biggest role, that there's a completely different message.

My background is advertising and marketing research. I spent the first 10 years of my [working] life in advertising and research, and I would be happy to go to my grave saying that we have never framed preparedness the way preparedness needs to be framed if you want people to do it.

No private-sector company would invest billions of dollars putting a message out that had such dismal returns. You just would never do it.

Different messengers and people need to hear the message from messengers that they believe in. I was just in a conversation about how religion influences disaster, and the reality is, if you want people who are affiliated with a religious group to get the message, they'll get that message when that religious organization threads it into the way they speak.

There are all kinds of ways to frame your conversation so that it works for the community.

The business community doesn't have a bunch of money to spend on this. The majority of businesses have not done any of the planning. It's the exception rather than the rule.

If you look at the big companies that've done it — the Targets and Wal-Marts — some of them only recently got into this game. Most businesses have done so little and there are really easy things they could do. Look at how cheap it is to have storage space online. You could back up your files so easily for pennies. If you don't have confidential information, you could back it up using Gmail because you have unlimited amounts of Gmail space.

Schools are a perfect example. Every time we do a presentation at a church, the people who line up to talk to us are almost always teachers. They are overwhelmed for what they're expected to do, so there are all sorts of things like having the kids play a much more active role in the planning and response.

jmckay@emergencymgmt.com

Lessons from Christchurch

Although the government structures are different, the U.S. can learn a lot from New Zealand's experience.

By Claire B. Rubin | Contributing Writer

Learning from experience, including that of other countries, is an important element of our knowledge about earthquakes and other disasters that affect major urban areas. The United States can learn from a recent report that assessed the response to the damaging earthquake that affected Christchurch and the surrounding Canterbury Region in New Zealand in February 2011.

The event's aftermath brought to the fore issues frequently faced in the U.S., such as how to scale up an emergency response, how to overcome organizational deficiencies and how to maintain continuity in a community that is suffering from major outages of power, water and sewage systems. Although New Zealand's form of government and governance system for emergency management differs from that found in the U.S., there is still much to learn from the New Zealand event.

The Facts

- Christchurch is a city of 348,000 where, during the middle of a workday, a magnitude 6.3 earthquake occurred. The epicenter was close to the city center, and the disaster was a complete surprise since there was no knowledge of a fault in that location.
- After strong ground shaking, as well as significant liquefaction and landslides, the impact on all sectors was high. Most of the city's central business district was damaged beyond repair, as was the hallmark cathedral in the city center. In addition, tens of thousands of local homes were damaged.
- This was the second major earthquake in the Canterbury Region within six months. The first occurred on Sept. 4, 2010, about

SHUTTERSTOCK.COM

Many of the buildings and infrastructure are still weakened from the earthquakes.

AFTER

25 miles west of Christchurch and, though it was a magnitude 7.1 earthquake, did not kill anyone.

- The Canterbury Region is still recovering from the September 2010 earthquake and some of the buildings and infrastructure are still weakened from the first quake. Response and recovery organizations also have had continuing problems.
- The city is a small island nation (with a population of 4.3 million people) whose nearest neighbor is more than 1,250 miles away. Mutual aid would have to come from a long distance.

2011 CHRISTCHURCH EARTHQUAKE BY THE NUMBERS

- 185 people were killed and 1,500 to 2,000 injured, 164 seriously.
- About 66 percent of businesses in Christchurch were affected, 20 percent of which had long-term damage from the earthquake.
- 220 building inspection teams assessed nearly 448,000 residential properties and found that:
- 5,000 properties were in the red zone *(not feasible to rebuild on the land at present time);*
- 10,000 were in the orange zone *(engineers must undertake further study)*; and
- 1,000 were in the gray zone *(homes can be repaired and rebuilt).*
- About 26,000 homes were vacant because they were unsafe for reoccupation or serious soil stability issues remained. *(These numbers changed over time and some zone names changed also.)*
- While the national electric grid survived, extensive damage occurred to local networks, with about 75 percent outage in Christchurch initially. However, power was restored to more than 50 percent in the first 24 hours.
- The water supply to more than 40 percent of residents was damaged, as was sewer service to about 50 percent of the population.
- Estimated total cost: $20 billion to 30 billion.

BEFORE

EN.WIKIPEDIA.ORG/ROGERWONG

The Report

Most of the information summarized thus far was taken from the recently released report commissioned by the New Zealand government. The report, Review of the Civil Defense Emergency Management Response to the 22 February Christchurch Earthquake, was conducted under a competitive contract sponsored by the country's Ministry of Civil Defence and Emergency Management.

Completed in June 2012 and released to the public on Oct. 4, the 243-page report provides a detailed account of the event and its impacts, focusing on the response phase. The assessment was done by a team of experienced, independent experts, with three representatives from New Zealand, one from Australia and one from the U.S.

The report covers the Ministry of Civil Defence Emergency Management (CDEM, the national agency responsible for disasters) response from the Feb. 22, 2012 earthquake to April 30, 2012. On that date, the response phase officially ended and the recovery process was taken over by the Canterbury Earthquake Recovery Authority. The stated purpose of the review was to "identify the practices that should be reinforced and identify the processes and policies that warrant improvements."

The report's major findings were:

- The duplication of control and EOCs between Christchurch city and the regional CDEM group was not only inefficient, but also put people and property at risk.
- Many people who were called upon to manage or staff the EOCs had neither the training nor the capability

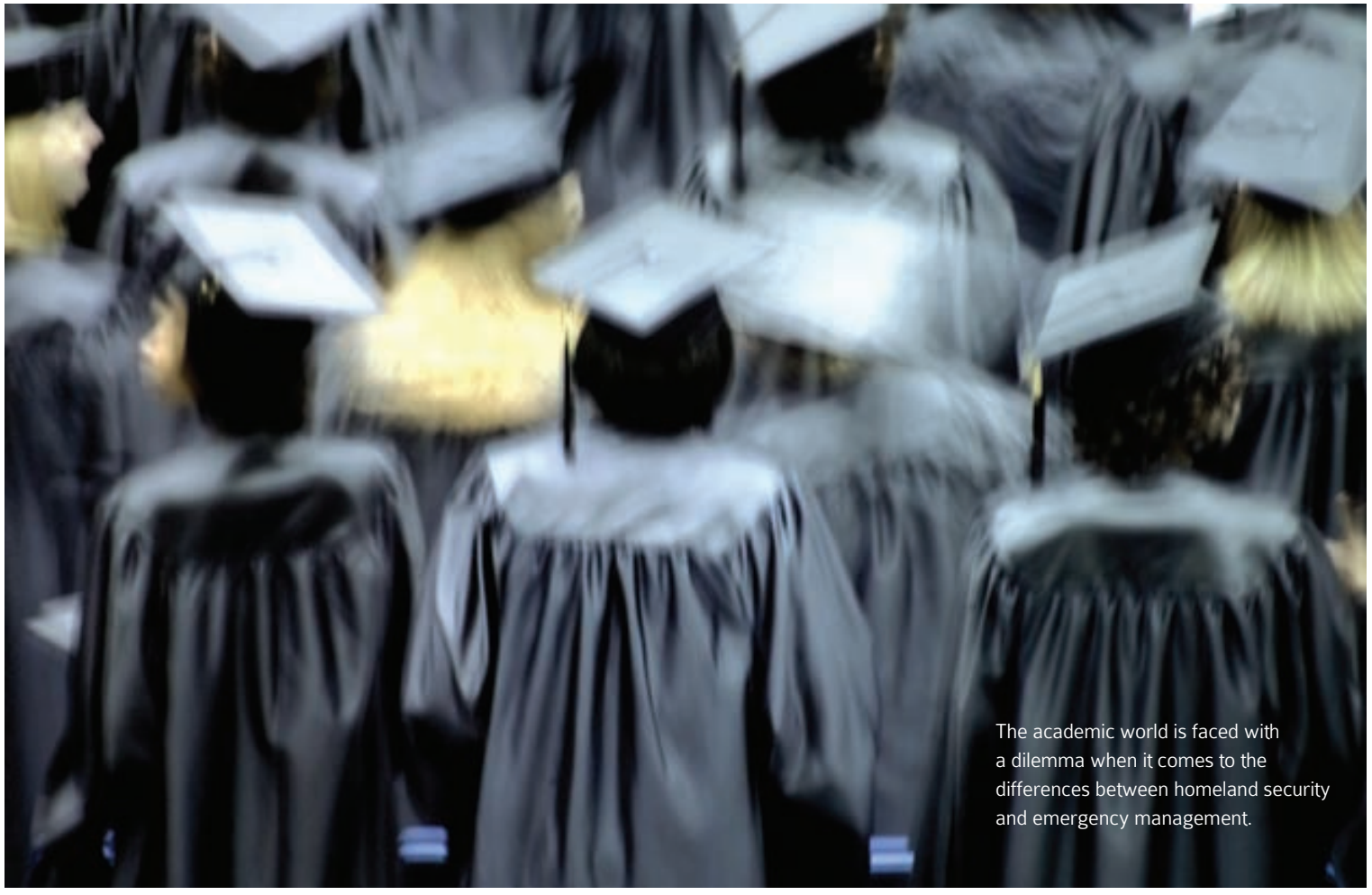
The **old Normal School Building** collapsed after a 6.3-magnitude earthquake on March 12, 2011 in Christchurch.

FEMA Deputy Administrator for Protection and National Preparedness **Tim Manning (left)** inspects the earthquake damage in Christchurch. *Photo by U.S. Embassy-New Zealand/Janine Burns/FEMA*

to lead during a major emergency, despite their skills to do other jobs in normal times.

- Community groups played a major part in the response, but two-way flows of information and provision of resources need to be improved.
- The needs of the business community and the preservation of jobs need to be made a specific objective during emergency response and emergency organization, and [the existing] structure needs modification to forge a better link.
- The position of the CDEM as a small element in the broad portfolio of the Department of Internal Affairs hampered its relationships with major departments in preparation for and during emergencies.
- One feature was strikingly apparent: Organizations of any kind that were well prepared in advance responded much better than those that were not.

Claire B. Rubin, a researcher and consultant in emergency management in the Washington, D.C., area, heads the firm Claire B. Rubin & Associates.



SHUTTERSTOCK.COM

The academic world is faced with a dilemma when it comes to the differences between homeland security and emergency management.

Sibling Rivalry

The emergency management and homeland security communities vie for supremacy in academia.

By Valerie Lucus-McEwen | Contributing Writer

Today's emergency management and homeland security practitioners often find themselves at an impasse in defining their individual responsibilities. If there is a clear line between what is considered to be a "homeland security" function or an "emergency management" function — or even what is common to both — it is still on the table for discussion.

This real-world dilemma between the boundaries is echoed in academia. When the DHS was created, a focus on terrorism pushed the concept of all-hazard disaster management to the back burner. Emergency management — having already developed higher education degrees, certifications, standards and associations — found itself struggling with homeland security for recognition, respect and funding.

As a result, colleges and universities scrambled after 9/11; it was a contest to attract students and DHS grant money. Somewhat abruptly, new students to the field and practitioners seeking additional education had a choice of degree programs or concentrations: one that emphasized creating resilient communities at a local level (emergency management); one geared to protect those communities from bad people at a national level (homeland security); or one with a little of both. The heated discussions about which degree had more significance were animated and intense.

"I call the gap between homeland security and emergency management 'sibling rivalry,'" said David McIntyre, a visiting fellow at the Homeland Security Studies and Analysis Institute (HSI) and director of Homeland Security and Defense Programs at the National Graduate School. "One is

RDPC
Rural Domestic Preparedness Consortium

Prepare For The Worst, Train To Be The Best

FEMA

AWR 209 Dealing with the Media: A Short Course for Rural Responders

Dealing with the Media: A Short Course for Rural First Responders is a six-hour, U.S. Department of Homeland Security approved training course designed to provide rural first responders with the skills and knowledge to quickly adopt the role of public information officer (PIO) if/when needed and to communicate with the public through the media.

Many rural first responder organizations do not have a full or part-time PIO on staff. In the event that a first responder is thrust into the role of PIO, it is important to understand how best to work with the available media outlets.

Through this course, rural first responders will gain an understanding of what the media is looking for at the scene of an emergency and in public awareness campaigns, as well as learn how to give interviews that work and write effective news releases.

Tuition-free for Qualifying Rural Jurisdictions

For more information or to schedule training contact RDPC at:
877-855-RDPC (7372) • info@ruraltraining.org • www.ruraltraining.org

Web-based version coming soon!

older than the other, one recently has been flashier in the news. But when you get right down to it, they are both family."

Nevertheless, beyond the conflict is a real dilemma for the academic side — whether to maintain and justify two similar but separate degree programs.

Focusing on Prevention

While academic degrees in emergency management have been flourishing for the past 15 years, homeland security degrees evolved as colleges and universities moved to fill national security needs in the aftermath of 9/11. Just as academia responded to World War II with courses in international relations, and the Cold War led to an increased emphasis on science and technology, academia responded to 9/11 with a curriculum that included topics such as intelligence analysis and critical infrastructure protection.

Consequently, homeland security degree and certificate programs exploded. The FEMA Higher Education Conference in June 2012 reported about 125 academic programs in homeland security, homeland defense, terrorism or terrorism-focused security studies. Stan Supinski, a former director with the Naval Postgraduate School and the Center for Homeland Defense and Security, and associate professor at Long Island University's Homeland Security Management Institute, puts that number higher when certificate programs are included. "When you consider that before 9/11, there were no programs called 'homeland security' and now there are between 350 and 400 — that is really incredible" he said.

Stan Supinski, associate professor at the Long Island University Homeland Security Management Institute, talks about the state of homeland security education last year.

NOVA SOUTHEASTERN UNIVERSITY

Supinski describes the early rifts between homeland security and emergency management as frustrating. "Emergency managers were saying this homeland security stuff is nothing new, just an added focus on terrorism," he said. "There are very clear distinctions that differentiate these fields of study, but there is also substantial overlap."

> "Emergency managers were saying this homeland security stuff is nothing new, just an added focus on terrorism. There are very clear distinctions that differentiate these fields of study, but there is also substantial overlap."

In Supinski's view, what primarily differentiates homeland security and emergency management is prevention, which was added as a separate, fifth component to the four traditional emergency management phases of mitigation, preparedness, response and recovery.

Prevention was added to the formula as part of the 2007 update of the National Fire Protection Association's NFPA 1600, Standard on Disaster/Emergency Management and Business Continuity Programs. Although the intent was to bring the standard into alignment with related disciplines, the addition was widely interpreted as trying to resolve the conflict between the all-hazards approach to emergency management and the need to enhance homeland security.

The intent wasn't entirely successful as practitioners on both sides of the emergency management/homeland security fence bristled at the idea that there were enough similarities to put them in the same community, much less the same family.

Community and Commonality

Community was a big part of the problem, according to McIntyre. "It is important to understand [emergency management and homeland security] were two different communities and were entirely ignorant of each other," he said. "And what happens when people don't know each other? Suspicion and hostility."

Reaction from academia to a need for community was scattered and the result was as convoluted as higher education can get. Existing emergency management or criminal justice programs were repurposed using existing curriculum, new courses were created, new degrees were approved. Progress made in building emergency management degree programs was discounted while processes already in place for developing

HOSTAGE RESCUE ONE DAY, VICTIM RECOVERY ANOTHER.

You're definitely not cut out for a desk job.

Dive/Rescue operations require top-of-the-line equipment. Brunswick Commercial and Government Products builds trailerable Impact RHIBs and unsinkable Boston Whalers specifically for dive professionals. Our boats feature unsurpassed load carrying capabilities, dive ladders, removable dive doors and ample equipment storage. Choosing BCGP to supply your boats will be the easiest decision you'll have to make all year.

Brunswick Commercial and Government Products, Inc.
386.423.2900 • brunswickcgp.com

Brunswick Commercial and Government Products (BCGP) is a division of Brunswick Corporation — the largest marine manufacturer in the world.

standards and core competencies stalled. The discussions about how different or similar the fields are was skipped altogether. Recently there has been a lot of backtracking to try to pick up all those missing pieces.

If there is any agreement about what is common in both fields, it is the criticality of knowing, understanding and appreciating each other. Most of the current degree programs feature introductory courses for both homeland security and emergency management. That is certainly a start.

"In the past few years, especially at the FEMA Higher Ed Conference, I'm really glad to see the two sides [emergency management and homeland security educators] come together," said Supinski. "I'm heartened by the atmosphere, the willingness to look across the aisle and recognize the fact that we all belong on the same side."

McIntyre agrees there is significant overlap between the two fields and it revolves around each side knowing neither can do its job without the other. "I don't ever think they will become a single community and for good reason," he said. "I don't want responders to set priorities based on what is best for the national economy. And I can't afford for national-level planners to be worried about how many fire trucks there are in Omaha."

The Role of Academia

If academia initially helped exacerbate the lack of community spirit between emergency management and homeland security, there are certainly things they could do now to help calm the waters. The first would be to recognize there is a core field curriculum with ample opportunities for specialization.

In his position with the Naval Postgraduate School, Supinski used a Venn diagram with three interlocking circles when he briefed university administrations wanting to develop their own homeland security degree programs. The circles represented national security affairs, public administration and emergency management. The intersection of those circles is the core knowledge that leads to a specialization in all the other areas. Academia generally missed that distinction, concentrating less on the core and more on the periphery.

One way to find community consensus would be to recognize that a higher education degree in either homeland security or emergency management should first be based in management and leadership skills, collaboration, familiarity with all kinds of hazards, and strategic as well as tactical thinking. Beyond that, and depending on the position, it may require knowledge as diverse as understanding the problems of border security in Arizona or the science of tsunamis in the Northwest.

Another important step academia could take to nurture community between homeland security and emergency management was high on McIntyre's list: invest the resources to create a cross-disciplinary program of study. He blames the universities for putting profit

first and refusing to invest in a broad faculty with the skills to address a combined program.

Higher education in this area is changing, but universities are still slow to recognize the value of practical experience. "We are seeing adult learners who want a combination of academic and applied instruction," McIntyre said. "It will be another generation before there is faculty with academic credentials and practical experience." In the meantime, programs that don't integrate educated practitioners — with or without a Ph.D. — just aren't going to flourish.

The problem McIntyre would "lay at the feet of DHS" is the failure in clearly stating what skills and education are necessary for people graduating and looking for jobs in either homeland security or emergency management. "We put a huge amount of federal effort in sorting out skills matrices and exercises and almost no time and thought into the linkage between education and work performance," he said.

The biggest distraction to creating an academic community around these two related fields is just semantics. In a dazzling display of sibling rivalry, proponents of both emergency management and homeland security stubbornly resist any consideration of a common label. The "name" debate makes the whole discussion as polarized as election-year politics.

"What would we call it?" Supinski asked. "That is a tough one. We are still going to have emergency managers and we are still going to have people who want to focus on homeland security."

McIntyre likes civil security to describe both camps because it helps clarify the fundamental difference between local and national security interests.

"The trick is that neither can be only one thing," McIntyre said. "If homeland security tries to create concepts and plans without regard for the emergency manager actually executing them, it is just a castle built on the wind. On the other hand, if emergency managers focus only on their own networks and not what is working its way down from the national level, they are going to be constantly surprised and disappointed when resources are funneled elsewhere."

The potential disconnect is obvious, yet few are stepping forward to offer a compromise — not DHS, as the major employer of both homeland security and emergency management professionals; not academia, as the provider of knowledge; and not the professionals out there taking care of business.

"The main point to emphasize is that the two really do go together," Supinski said. "Once we can come to some agreement on that, our whole community will benefit and we can grow together the way we should have been all along."

Valerie Lucus-McEwen is a certified emergency manager and certified business continuity professional. She also writes the Disaster Academia blog for *Emergency Management* at www.emergencymgmt.com/academia.

MASTER OF SCIENCE IN EMERGENCY SERVICES MANAGEMENT

YOU CAN. YOU WILL.

Earn your degree online!

WHY CSU?

- Affordable Tuition
- Complimentary Tutoring Services
- No ACT, SAT, GMAT or GRE Required
- Self-paced or Structured Learning
- TA and VA Benefits
- Textbooks at No Cost
- No Application Fee

OTHER ONLINE DEGREES

- Associate of Applied Science in Fire Science
- Associate of Applied Science in Criminal Justice
- Bachelor of Science in Fire Science
- Bachelor of Science in Criminal Justice
- Bachelor of Science in Occupational Safety & Health Concentration in Fire Science
- Master of Science in Occupational Safety & Health
- Master of Science in Criminal Justice

Visit Us Online for More Information!

COLUMBIA SOUTHERN UNIVERSITY

Online Degrees. Low-Cost Tuition. Superior Service.

www.ColumbiaSouthern.edu/ESM | 800.977.8449

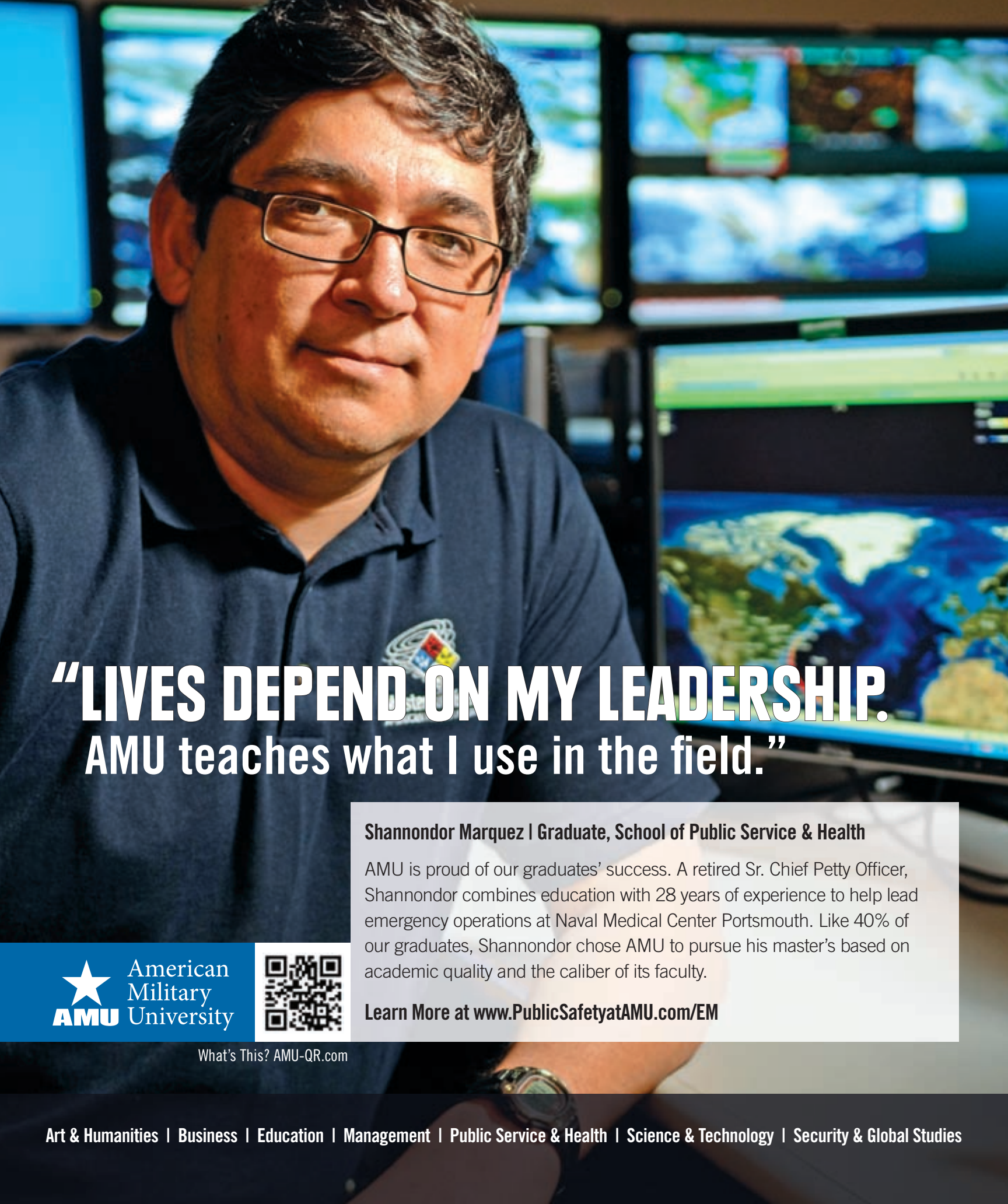
Visit our website at www.ColumbiaSouthern.edu/Disclosure for information about gainful employment including cost of attendance, on-time graduation rates, occupational opportunities, median student debt and other important information about CSU programs.

Homeland Security Bachelor's Degree Programs

INSTITUTION	PROGRAM	CONTACT	PHONE	E-MAIL
American Public University	BA Homeland Security	Dr. Chris Reynolds	877-755-2787	creynolds@apus.edu
Capella University	BS Public Safety- Emergency Management	Charles M. Tiffin	612-977-4120	charles.tiffin@capella.edu
Central Pennsylvania College	BS Homeland Security Management	Samuel W. Morgan	717-728-2247	samuelmorgan@centralpenn.edu
Colorado Technical University	BS Criminal Justice- Homeland Security/Emergency Management	Richard Holloway	224-293-5848	rholloway@ctuonline.edu
Corinthian Colleges	Bachelor's in Homeland Security	Daniel Byram	714-427-3000 x201	dbyram@cci.edu
Eastern Kentucky University	BS Homeland Security	Dr. Kay Scarborough	859-622-1464	kscarbocop@aol.com
Herzing College	BS Homeland Security and Public Safety	Mary Beth Robbins	205-916-2800	maryb@bhm.herzing.edu
National University	BS Domestic Security Management	Chandrika Kelso	858-642-8433	sviswana@nu.edu
Savannah State University	BA Homeland Security and Emergency Management	Emily Bentley		bentleye@savstate.edu
Southwestern College	BS Security Management	Kara Norris	888-684-5335	kara.norris@sckans.edu
Thomas Edison State College	BS Homeland Security and Emergency Management	Office of Admissions	888-442-8372	info@tesc.edu
Tiffin University	BS Criminal Justice-Homeland Security	Allen Smith	419-488-3395	smithra@tiffin.edu
Tulane University	Bachelor's in Homeland Security	Keith Amacker	504-247-1662	kamacker@tulane.edu
University of Alaska, Fairbanks	Bachelor's of Emergency Management	Cameron Carlson	907-474-6537	cdcarlson@alaska.edu
University of Maryland University College	BS Homeland Security	Stephen S. Carter	240-684-2875	sscarter@umuc.edu
Vincennes University	BS Homeland Security and Public Safety	Louis J. Caprino	812-888-6830	LCaprino@vinu.edu
Virginia Commonwealth University	BA Homeland Security and Emergency Preparedness	Dr. William Newmann	804-828-8038	wnewmann@vcu.edu

Homeland Security Programs Bachelor-Level Concentrations

INSTITUTION	PROGRAM	CONTACT	PHONE	E-MAIL
American Intercontinental University	BS Criminal Justice-Homeland Security/Crisis Management	John Campbell	224-293-5684	jcampbell@aiuniv.edu
Austin Peay State College	BS Criminal Justice-Homeland Security for Law Enforcement	Thomas R. O'Connor	931-221-1477	oconnort@apsu.edu
Drexel University	Certificate or Minor in Emergency Management	Alan Dorfman	215-895-0948	bad37@drexel.edu
East Carolina University	Minor in Security Studies	Dr. Rick Kilroy	252-328-2349	kilroy@mail.ecu.edu
Embry-Riddle Aeronautical University	BS Homeland Security-Homeland/Cyber-Security	James D. Ramsay	386-226-7153	James.Ramsay@erau.edu
Excelsior College	BS Criminal Justice-Homeland Security	John J. Greene	518-464-8669	jgreene@excelsior.edu
Empire State College Center	BS Homeland Security, Emergency Management or Fire Services	Jim Savitt	518-587-2100 x2410	Jim.Savitt@esc.edu
Grantham University	BS Criminal Justice-Homeland Security	Gary Sutter	816-448-3681	sutterg@grantham.edu
Indian River State College	BS Organizational Management-Public Safety & Homeland Security	Stephen Huntsberger	772-462-7945	shuntsbe@irsc.edu
Louisiana State University	BA Liberal Arts-Disaster Science and Management	John C. Pine	225-578-1075	jpine@lsu.edu
Mountain State University	BS Criminal Justice-Homeland Security	Michael J. Kane	304-929-1308	mkane@mountainstate.edu
Northeastern State University	BS Criminal Justice-Homeland Security	James Hall	918-449-6551	halljb@nsuok.edu
SUNY- Maritime College	Minor in Transportation Security	Admissions	718-409-7341	conted@sunymaritime.edu
Ohio State University	International Studies-Security & Intelligence Specialization	Karlene S. Foster	614-292-9657	foster.24@osu.edu
University of Central Florida	Minor in Emergency Management & Homeland Security	Dr. Claire Knox	407-823-2604	cknox@mail.ucf.edu
Walden University	BS Criminal Justice – with specialization in Homeland Security	Enrollment Adviser	866-492-5366	info@waldenu.edu


"LIVES DEPEND ON MY LEADERSHIP.
AMU teaches what I use in the field."
Shannondor Marquez | Graduate, School of Public Service & Health
AMU is proud of our graduates' success. A retired Sr. Chief Petty Officer, Shannondor combines education with 28 years of experience to help lead emergency operations at Naval Medical Center Portsmouth. Like 40% of our graduates, Shannondor chose AMU to pursue his master's based on academic quality and the caliber of its faculty.
Learn More at www.PublicSafetyatAMU.com/EM
AMU American Military University
What's This? AMU-QR.com
Art & Humanities | Business | Education | Management | Public Service & Health | Science & Technology | Security & Global Studies

Homeland Security Doctoral Programs

INSTITUTION	PROGRAM	CONTACT	PHONE	E-MAIL
Capella University	Doctor of Philosophy-Public Safety w/Emergency Management	Charles Tiffin	612-977-4120	Charles.Tiffin@Capella.edu
Colorado Technical University	Doctor of Management-Homeland Security	Richard Holloway	224-293-5848	rholloway@ctuonline.edu
Northcentral University	Doctor of Philosophy-Business Administration w/Homeland Security	Francisco C. Lopez	850-304-3745	flopez@ncu.edu
Saint Louis University	Doctor in Biosecurity and Disaster Preparedness	Larry Bommarito	314-977-8135	bommarlg@slu.edu
Walden University	PhD Public Policy & Admin.-Homeland Security Policy & Coordination	Enrollment Adviser	866-492-5336	info@waldenu.edu

Homeland Security Master's Certificate Programs

INSTITUTION	PROGRAM	CONTACT	PHONE	E-MAIL
California University of Pennsylvania	Master's in Legal studies with Homeland Security track	Dr. Charles P. Nemeth	724-597-7400	nemeth@calu.edu
Drexel University	Graduate Certificate in Homeland Security Management	Brandon Alan Dorfman	215-895-0948	bad37@drexel.edu
Fairleigh Dickinson University	MS Homeland Security	Paulette Laubsch	201-692-6523	plaubsch@fdu.edu
IUPUI	Graduate Certificate in Homeland Security and Emergency Mgmt	Thomas Stucky	317-274-3462	tstucky@iupui.edu
Jacksonville State University	MS in Emergency Management	MS. Denise Dasilva	256-782-8268	ddasilva@jsu.edu
Long Island University	Graduate Certificate in Emergency Management	Vincent E. Henry	631-287-8010	Vincent.Henry@liu.edu
Missouri State University	Graduate Certificate in Homeland Security	Dr. Bernard McCarthy	417-836-6679	bernardmccarthy@missouristate.edu
Northcentral University	MBA Homeland Security	Francisco C. Lopez	850-304-3745	flopez@ncu.edu
Pennsylvania State University World Campus	Intercollege Master of Professional Studies (iMPS) in Homeland Security	Dr. Jeremy Plant	814.865.5403	pennstateonline@psu.edu
Rutgers University	Graduate Cert in Transportation Mgmt: Vulnerability, Risk & Security	Judith Auer Shaw	732-932-5475	judy.shaw@rutgers.edu
University of Central Florida	Graduate Certificate in Emergency Mgmt and Homeland Security	Dr. Claire Knox	407-823-2604	cknox@mail.ucf.edu
University of Massachusetts, Boston	Graduate Certificate in Global Post-Disaster Studies	Adenrele Awotona	617-287-7116	Adenrele.Awotona@umb.edu
Walden University	MS Public Policy, Emergency Management and Criminal Justice	Enrollment Adviser	866-492-5336	info@waldenu.edu

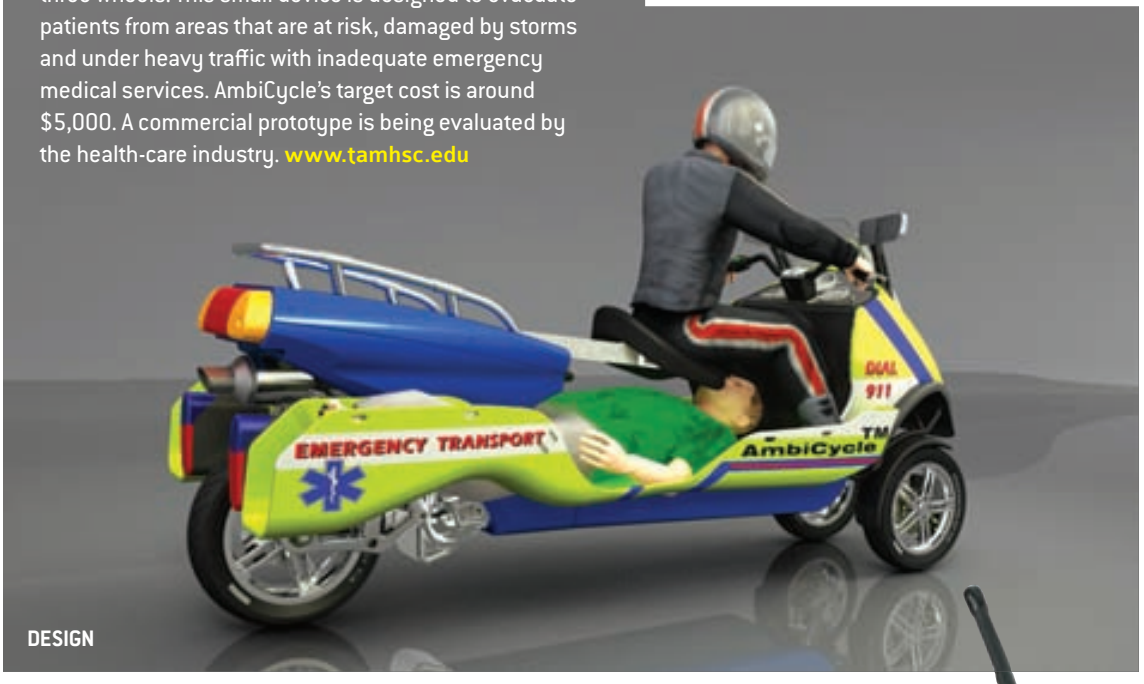
Homeland Security Master's Programs

INSTITUTION	PROGRAM	CONTACT	PHONE	E-MAIL
American Public University	MA Homeland Security	Dr. Chris Reynolds	877-755-2787	creynolds@apus.edu
Arkansas Tech University	MS Emergency Management and Homeland Security	Ed Leachman	479-964-0536	eleachman@atu.edu
Bellevue University	MS Security Management	Therese Michels	402-557-7116	Therese.Michels@beelevue.edu
Capella University	MS Public Safety with Specialization in Emergency Mgmt	Charles Tiffin	612-977-4120	Charles.Tiffin@Capella.edu
Colorado Technical University	MS Management-Homeland Security	Richard Holloway	224-293-5848	rholloway@ctuonline.edu
Eastern Kentucky University	MS Safety, Security and Emergency Management	Thomas D. Schneid	859-622-2382	Tom.schneid@eku.edu
George Mason University	M Public Administration EM & Homeland Security	Paul Posner	703-993-3957	pposner@gmu.edu
Johns Hopkins University	MA in Government with Homeland Security Emphasis	Dorothea I. Wolfson	202-452-1123	dorotheawolfson@jhu.edu
Long Island University	MS Homeland Security Management	Vincent E. Henry	631-287-8010	Vincent.Henry@liu.edu
National University	MS Homeland Security and Safety Engineering	Dr. Shedar Viswanathan	858-642-8416	sviswana@nu.edu
Northcentral University	MBA Homeland Security	Francisco C. Lopez	850-304-3745	flopez@ncu.edu
Penn State University-Online	Master of Homeland Security in Public Health Preparedness	Robert Cherry	717-531-6066	rcherry@psu.edu
Rochester Institute of Technology	MS: Counterterrorism, WMD Threat Assessment & Defense or cyber-security	Maureen Valentine	585-475-7318	emermgmt@mail.rit.edu

Alternative Ambulance

Ambulances in the U.S. are typically around 13 feet long, eight feet high and struggle to maneuver through congested traffic. Doctors at the Texas A&M Health Science Center School of Rural Public Health are developing an alternative to the traditional ambulance. Called the **AmbiCycle**, it resembles an elongated motorcycle with three wheels. This small device is designed to evacuate patients from areas that are at risk, damaged by storms and under heavy traffic with inadequate emergency medical services. AmbiCycle's target cost is around $5,000. A commercial prototype is being evaluated by the health-care industry. www.tamhsc.edu

PROTOTYPE



DESIGN

Multimedia Call Handling

Impact 360 for Public Safety Powered by Audiolog is a packaged solution from Verint Systems that brings multimedia recording together with key functionality for enhancing performance in 911 centers, including quality assurance, performance management, incident investigation and analytics, speech analytics, workload forecasting and staff scheduling, staff coaching and training, and citizen surveys. This flexible, easy-to-use solution can help organizations comply with best practices on call handling evaluation and reporting — including those arising from next-generation 911. **www.verint.com**

TOUGH CALL

Harris Corp. released the InTouch RPC-200, what it's calling the first Android-based ruggedized long term evolution (LTE) smartphone designed for public safety field use. The phone operates on both public safety band 14 LTE and commercial 2G/3G/4G cellular networks. It features HDMI video and a 5-megapixel camera on a hardened 4-inch display. The InTouch was designed with a large push-to-talk button, waterproof speaker and noise-cancellation capability for on-scene performance. www.harris.com

TOSS AWAY

High-risk operations and surveillance missions will get a boost with the Throwbot XT, a mobile micro-robot that provides audio and video reconnaissance. Made by Recon Robotics, the Throwbot XT is water and dust resistant, weighs 1.2 pounds and can be thrown up to 120 feet. It's equipped with an infrared optical system and operated with a handheld unit. www.reconrobotics.com

HOMELAND SECURITY CERTIFICATE PROGRAM

Courses for public safety practitioners.
Courses include:

- **Law Enforcement Professionals**
  Available Now!
- **Fire Service Professionals**
  Available Now!
- **Emergency Management Professionals**
  Coming Soon!

No fees, no cost!
Enroll in a course today at
www.preventivestrategies.net.

Homeland Security

RDPC
Rural Domestic Preparedness Consortium

DISCLAIMER: This project was supported by Cooperative Agreement Number 2006-GD-T6-K001 administered by the U.S. Department of Homeland Security/FEMA, Training and Exercises Integration Secretariat. Points of view or opinions in this document are those of the author and do not represent the official position or policies of the U.S. Department of Homeland Security.

To enroll or get more information
please visit **www.preventivestrategies.net**
or call 1-800-860-6657.

Institute for Preventive Strategies
The Center for Rural Development

By Eric Holdeman

Market Like Coca-Cola

September was National Disaster Preparedness Month. Many emergency management programs are now working on other mission areas that might include disaster planning or exercises. But the month of emphasis on preparedness is over, and we won't concentrate on the topic again until next year.

Is this the right thing to do? Should we have one month of preparedness and 11 months of maintenance messaging on the topic of becoming prepared for disasters? We need to change this mentality.

I DON'T BELIEVE THE NATIONAL SURVEYS THAT TOUT THAT UPWARD OF 30 TO 40 PERCENT OF THE GENERAL POPULATION IS PREPARED FOR A DISASTER.

No matter how prepared you become as a single government or coalition of governments, you can't overcome the lack of disaster preparedness by your general population if the event is catastrophic. No matter how many government resources you throw at problems, there isn't enough mutual aid or Emergency Management Assistance Compact aid to overcome the hole that has been dug by having your citizens and businesses unprepared for a disaster.

While the general message in the past has been to become prepared for three days or 72 hours, most people, emergency managers included, are not ready to be on their own for even three hours. I don't believe the national surveys that tout that upward of 30 to 40 percent of the general population is prepared for a disaster. It just can't be true based on my own personal experience in talking with individuals and families.

What's needed to overcome this woeful lack of disaster preparedness is a national-level campaign that is continuous and never-ending in encouraging and motivating people to become prepared for the next disaster. And three days is not enough.

Look at how Coca-Cola is advertised. We know Coke is sold using polar bears and Santa Claus as marketing mascots, and the symbol of Coke is emblazoned on our brains so that we can mentally recall what the logo looks like.

And yet we will keep seeing Coca-Cola advertised continuously using television, radio, billboards, magazine ads, bus signs, the Internet and yes, even social media because otherwise people won't buy it.

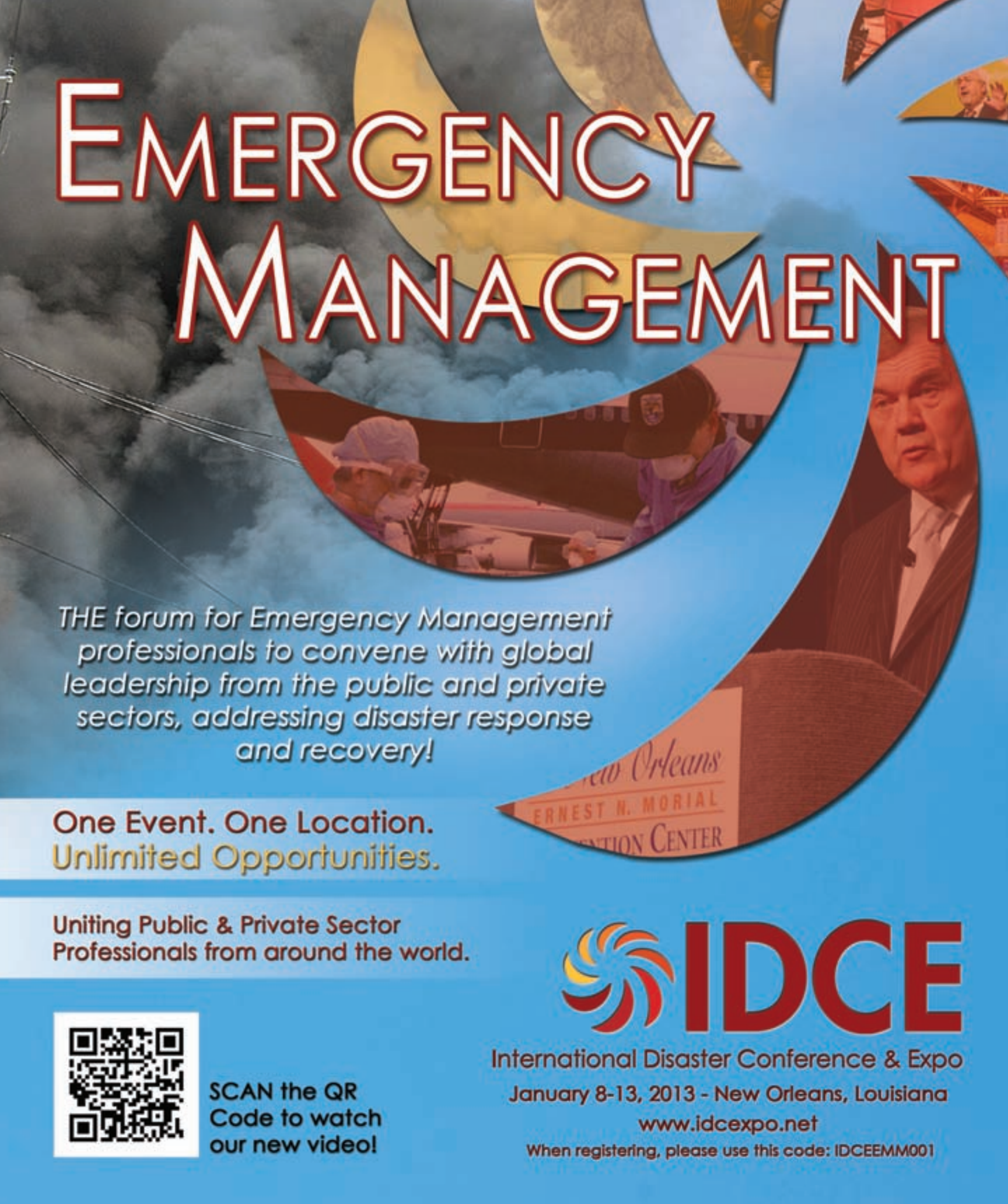
About a month ago, I heard a professional public relations leader explain that his agency did what it could with the funding it was given. He remarked that it would take millions of dollars to do a national advertising campaign like major corporations do.

OK, let's do some basic math — it's been 10 years since the advent of homeland security grants. Those averaged $3.2 billion per year for state and local preparedness. So we've spent roughly $32 billion on "stuff" and very little on disaster preparedness messaging. I fought tooth and nail to get funds allocated to that mission for my own homeland security region. We got some $2.5 million over a number of years that we translated into more than $5 million in advertising on television, radio, billboards and buses in a partnership with the Seattle Mariners baseball team.

What if, instead of trying to get the Ad Council to support disaster preparedness messaging, we worked with the national networks to buy air time and get our disaster preparedness message to everyone in the U.S? Not for a month, but continuously. There could be major ad buys in national magazines, we could target women and children to motivate them to become prepared for disasters and to maintain a level of preparedness for their own welfare and that of their community. This isn't rocket science — we know how to do it. We have the messages, the means and the wherewithal to make a huge impact for disaster preparedness.

We need to sell disaster preparedness like they sell Coca-Cola.

ERIC HOLDEMAN IS THE FORMER DIRECTOR OF THE KING COUNTY, WASH., OFFICE OF EMERGENCY MANAGEMENT. HIS BLOG IS LOCATED AT WWW.DISASTER-ZONE.COM.


EMERGENCY
MANAGEMENT
THE forum for Emergency Management professionals to convene with global leadership from the public and private sectors, addressing disaster response and recovery!
One Event. One Location.
Unlimited Opportunities.
Uniting Public & Private Sector Professionals from around the world.
SCAN the QR Code to watch our new video!
IDCE
International Disaster Conference & Expo
January 8-13, 2013 - New Orleans, Louisiana
www.idcexpo.net
When registering, please use this code: IDCEEMM001

By Charlotte Franklin

Supply Chain Management

When communities face a disaster or civil emergency, the government and private sector must work together to move swiftly and smoothly into response and recovery modes. But when dealing with the effects of hurricanes, floods, tornadoes or man-made events, some communities will experience unexpected challenges over the logistics and distribution of resources like water, food and medical supplies.

One solution is to look at emergency management and disaster recovery as a supply chain issue instead of an inventory issue. This way, emergency managers and communities are more effectively and efficiently positioned to handle a crisis before an incident occurs. Another reason for this view is that it will open up opportunities to find solutions that allow for faster, more efficient delivery of critical supplies once an incident happens. The key to this approach is a new conversation in which local government asks private businesses, "How can we clear the way for the delivery of emergency resources should an incident occur?"

We know that businesses already have the expertise and processes to move supplies into the community. They are the recovery and continuity experts. When the needed types of supplies change depending on a disaster, delivery and distribution challenges remain consistent, even if the scale changes.

When the emergency happens, it's too late for planning. Putting the emphasis on mitigating supply chain vulnerabilities before a crisis can help remedy major challenges related to disaster recovery resource management:

1. **There's always a period immediately after an incident when response is the priority.** Once response initiates, recovery can begin, but only if supply destination options have been preplanned so the right supplies are already on their way.
2. **The private and nonprofit sectors are going to help.** Local emergency managers can work with them pre-event to pave their way and address regulatory and policy-related obstacles that may impede their progress.
3. **The level of community resiliency can only be truly evaluated after the incident by measuring recovery time length and its efficiency.** Given this, local emergency management should ensure supply chain resiliency is a top priority.
4. **Until now, pre-event recovery resource planning has been mostly about inventory and warehousing.** But with an emergency, knowing precisely what will be needed where, in what quantity and by whom, can't be predicted. Focusing on the supply chain redundancy, as well as real-time communication and interface, can provide a more effective way to get critical supplies quickly after an incident.
5. **Recovery resource distribution planning will expose where intersections already exist between for-profit supply delivery systems and a community's nonprofit services, so as not to reinvent the process.**
6. **On Jan. 30-31, 2013, Arlington County, Va.**, will host the Local Capacity Supply Chain Exercise Summit, which will unite grocers, retailers, financial institutions, medical suppliers, supply chain experts and the critical infrastructure stewards that support them. Recommendations from the summit will be made available to all communities as a guide for a supply chain-focused approach to emergency preparedness.

In addition, a major expansion of our Public Recovery Resource Access Portal is under way to add more mapping layers and expand the jurisdictions that can use it. This online resource provides real-time updates during disasters to help businesses and the public know where to donate and receive supplies. It has been designed to be easily adapted to any jurisdiction.

CHARLOTTE FRANKLIN IS THE DEPUTY COORDINATOR OF ARLINGTON COUNTY, VA.'S OFFICE OF EMERGENCY MANAGEMENT. TO ATTEND THE TWO-DAY SUMMIT, EMAIL HER AT CFRANKLIN@ARLINGTONVA.US OR CALL (703) 228-0593.

Preparation is everything

Emergency Operations Center solutions that make a difference, when every second counts.

millenniuminc.com/eoc

One Point of Contact.
Endless Possibilities.

Millennium Communications Group has the expertise and experience to provide cutting-edge designs and solutions for Emergency Operations Centers. With technology innovations that will aid emergency management, we are your single point of contact for emergency preparedness solutions.

MILLENNIUM
COMMUNICATIONS GROUP INC.

800.677.1919 | info@millenniuminc.com

GSA
Contract Holder
Contract #GS-35F-0220R

THE RIGHT TECHNOLOGY TO RESPOND FASTER.

MAKE A DIFFERENCE FOR YOUR AGENCY WITH THE RIGHT EXPERIENCE, NETWORK AND STRATEGIC ALLIANCES.

VERIZON SOLUTIONS FOR PUBLIC SAFETY

- MONITORING & CONTROL
- MOBILE PUBLIC SAFETY
- INTEROPERABILITY
- DISASTER RECOVERY
- TELEMATICS

Verizon technology enables public safety solutions that facilitate interoperability, allowing your agency to exchange critical information with public safety agencies, doctors in facilities and emergency responders in the field. Through innovative Advanced Communications solutions, Verizon helps emergency response teams access the data they need to stay informed and better prepared to respond to any situation. And it's all made possible with the security and reliability of America's largest 4G LTE network.

Start making a difference for your agency.
Visit: verizonwireless.com/publicsafety

verizon

Cyber & Physical Security Special Report

A RESEARCH REPORT FROM THE
CENTER FOR DIGITAL GOVERNMENT

WHEN WORLDS COLLIDE

The Converging Threats to Governments' Cyber and Physical Infrastructure

MARK WEATHERFORD & SUZANNE SPAULDING,
U.S. DEPARTMENT OF HOMELAND SECURITY

A SUPPLEMENT TO EMERGENCY MANAGEMENT/GOVERNMENT TECHNOLOGY

Work anywhere, security everywhere.

AT&T has solutions to protect constituent data, no matter where it is – in a pocket, on a desk or dwelling in a data center.

State and local governments can count on AT&T's legendary reliability to provide both security and solutions to support and protect your agency.

Rethink how government does business inside the network of possibilities from AT&T.

To find out how, visit att.com/secureworkforce

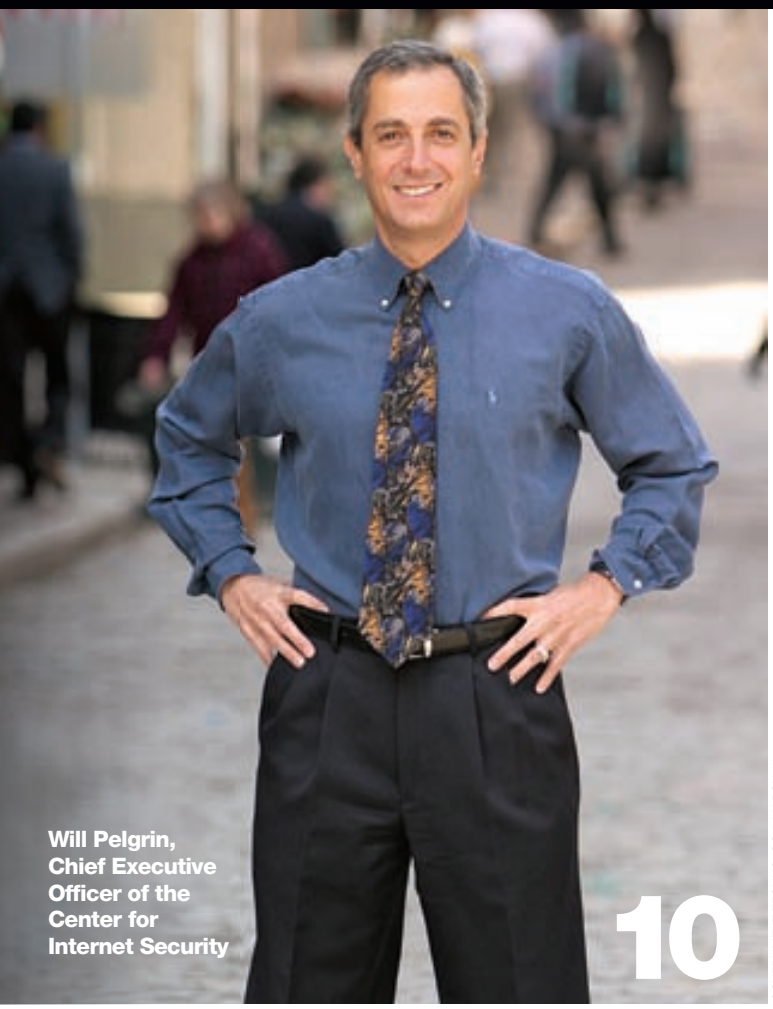
VULNERABLE

PROTECTED

Rethink Possible®

Download the free scanner app at http://scan.mobi and scan this code to learn more.

CONTENTS



Will Pelgrin, Chief Executive Officer of the Center for Internet Security

10

GOVERNMENT TECHNOLOGY, MARCH 2011

A member of Anonymous, a hacktivist group.

13

FLICKR/STEPHEN C. WEBSTER

e.Republic SMART MEDIA FOR PUBLIC SECTOR INNOVATION

100 BLUE RAVINE ROAD, FOLSOM, CA 95630
916.932.1300 PHONE | 916.932.1470 FAX

COVER PHOTO BY BOB RIVES

Alarm Bells

Agencies must act now to protect infrastructure

TOM MCKEITH

> "The collective result of these kinds of attacks could be a cyber Pearl Harbor."
>
> — Leon Panetta
> U.S. Defense Secretary

It wasn't that long ago that the greatest cyber threat we had to worry about was a twelve-year-old kid in a basement, playing on a desktop computer and enjoying being called a "hacker." Flash forward several years and not only have the threats multiplied, they have also become significantly more menacing.

Cyber crimes such as identity theft and other malicious activities are rampant as sophisticated criminal networks around the world are learning how to make money virtually without using a physical weapon. Ratchet it up another notch and now nation states — those counted in the "friendly and enemies" columns — are using digital pathways to conduct espionage and to steal information from governments and businesses. This data can be used to enrich their own industries or to hunt for weaknesses and system vulnerabilities that can be potentially exploited in the future.

There is a cyber Cold War developing as countries plot to do great physical harm to critical infrastructures and other systems such as banking. Millions of attacks each week seek to disrupt our digital networks, which could have huge impacts to systems and processes. Recently, U.S. Defense Secretary Leon Panetta remarked, "The collective result of these kinds of attacks could be a cyber Pearl Harbor."

Alarm bells are ringing in Washington, D.C., as the federal government seeks to alert governments and businesses that they must act now to better protect their digital infrastructure. Our defense must be a collaborative one because of the interdependencies between our systems and the supporting critical infrastructure. The weakest link is the one that can cause a cascading impact across a broad swath of our nation.

This Special Report highlights recent research by the Center for Digital Government, as well as case studies and best practices to help you better prepare and defend your organization from the inevitable cyber and physical attacks that are looming on the horizon. We hope you find it helpful in developing strategies to better prepare your organization for potential future threats.

Marty Pastula
Vice President, Emergency Management and Homeland Security, e.Republic

Whether deploying unified communications across your organization or looking for better ways to serve your customers and community, NEC can help you do more with less - and maintain peace of mind in the process. To find out how, visit us online at necam.com/government

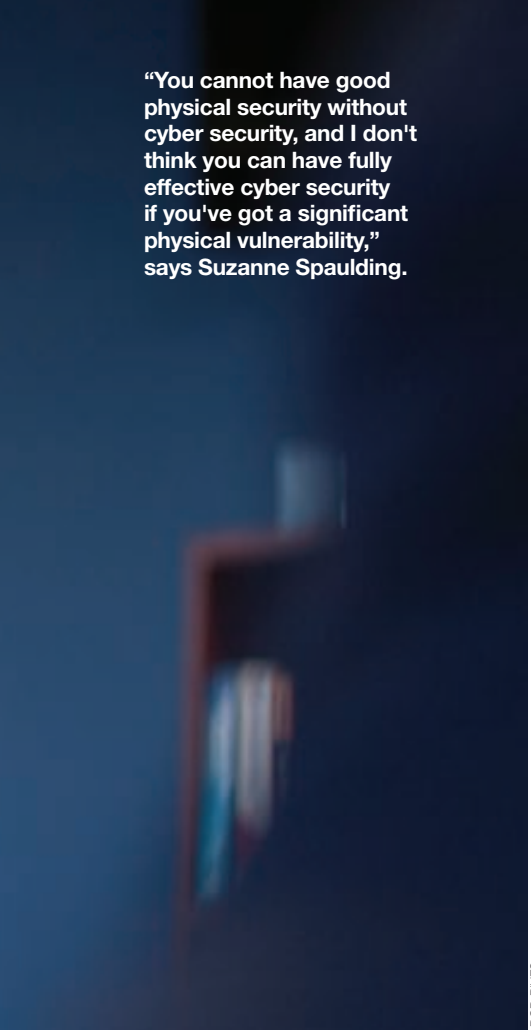
Empowered by Innovation NEC

Playing Defense

Security threats to government resources are ever-present — and increasingly sophisticated.

It's no secret that state and local agencies are under siege these days — what's hard to comprehend is how much. Before hackers compromised the personal information of 500,000 Utah citizens earlier this year, the state was enduring almost a million attacks *each day* to its IT network. In April, someone — possibly from as far away as Eastern Europe — made it through the defenses. When the digital dust cleared, more than a quarter million Social Security numbers were stolen, along with patient health data and a variety of other sensitive information. It cost a highly regarded state CIO his job and forced the governor to acknowledge that the state "failed to honor" the commitment to protect the personal information of its citizens.[1]

Unfortunately, this was far from an isolated case. States and municipalities around the country are becoming inundated with security assaults. Nevada's Chief Information Security Officer Christopher Ipsen declines to give an exact number, but he acknowledges that his state, like Utah, is also logging nearly a million daily attacks on its highly valuable information and IT resources.[2] Reports from other IT professionals at state and local agencies across the country tell a similar tale. In an exclusive new survey conducted by the Center for Digital Government (CDG), senior IT and security department decision-makers report that attacks are ever-present — and growing in numbers — in the public sector. For example, 60 percent of the survey respondents said their agency experienced some form of cyber threat or intrusion in the past year. Added to that, two-thirds



"You cannot have good physical security without cyber security, and I don't think you can have fully effective cyber security if you've got a significant physical vulnerability," says Suzanne Spaulding.

BOB RIVES

also fended off some form of physical threat. These professionals don't expect the situation to change anytime soon. Eighty-one percent are bracing for cyber threats to rise over the next year, while 51 percent expect physical threats will also increase in the same period.[3]

The new research also revealed something interesting behind the numbers — today's attackers are far from being a monolithic group that is easy to profile and defend against. Instead, the threats come from people and organizations that represent widely diverse resources and motives. "Foreign countries trying to sabotage or access the digital infrastructure" was a common refrain of security officials when asked to describe the biggest cyber threats. "Criminal elements who use the Internet to gain profit," "groups related [to] or belonging to Anonymous," "domestic terrorism" and even "careless employees" were other common themes cited among those surveyed.

What is clear from these statistics and anecdotes is that security professionals at state and local organizations can no longer only rely on cyber and physical security strategies that revolve around installing the latest anti-virus software and firewalls while locking down facilities with smart cards and uniformed guards. The defenses must grow in sophistication as each new threat emerges, and security strategies require a higher level of coordination than ever between groups responsible for protecting IT resources and those working to keep intruders outside of protected facilities.

"You cannot have good physical security without good cyber security, and I don't think you can have fully effective cyber security if you've got a significant physical vulnerability," says Suzanne Spaulding, deputy undersecretary for the National Protection and Programs Directorate at the U.S. Department of Homeland Security.[4]

Coordination may be important, but it's not always easy. One fundamental challenge agencies face is how to clearly delineate who is responsible for each of the security measures needed to address today's biggest vulnerabilities. The "who" used to be clear — IT technicians handled cyber security, while facilities managers and specialists, who often had a law enforcement background, addressed physical safeguards. But the lines are blurring, thanks in part to new technologies permeating core safeguards like video surveillance systems, which leave many agencies trying to catch up to not only the latest threat but also emerging best practices for securing their entire operations.

Coordination may be important, but it's not always easy. One fundamental challenge agencies face is how to clearly delineate who is responsible for each of the security measures needed to address today's biggest vulnerabilities.

Fortunately, state and local security officials can benefit from one aspect of today's cyber and physical threat environment — strength in numbers. Far from facing these risks alone, agencies of all sizes can draw on lessons learned — and shared — by their peers, along with a steady stream of commercial innovations from security solutions companies. This report will drill into these best practices, offer case study highlights of successful security policies across the country, report additional details from the latest CDG research and provide a list of the top tools available today to defend against the shadowy community of domestic and international intruders. The sad truth is that no security plan is foolproof — but an aggressive and coordinated approach can limit the damage and honor the commitment state and local agencies have to protect the public's personal information.

State and local governments are on the front lines when it comes to stopping today's biggest threats to cyber and physical resources. They're also not shy when it comes to identifying top risks and why stopping them can be such a challenge.

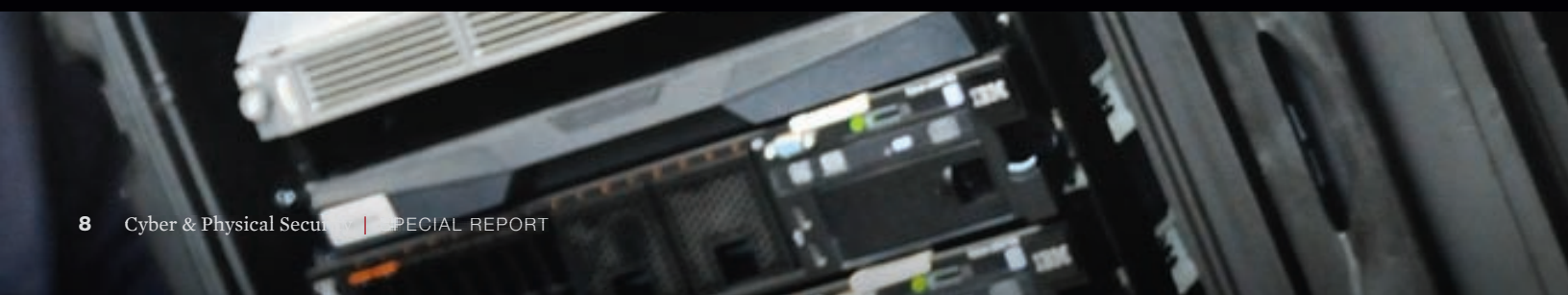
The Center for Digital Government surveyed 100 senior government IT and security decision-makers for this report. Their answers to questions presented in the survey are reflected on this page. Quotes from the survey remain anonymous to encourage open discussion.

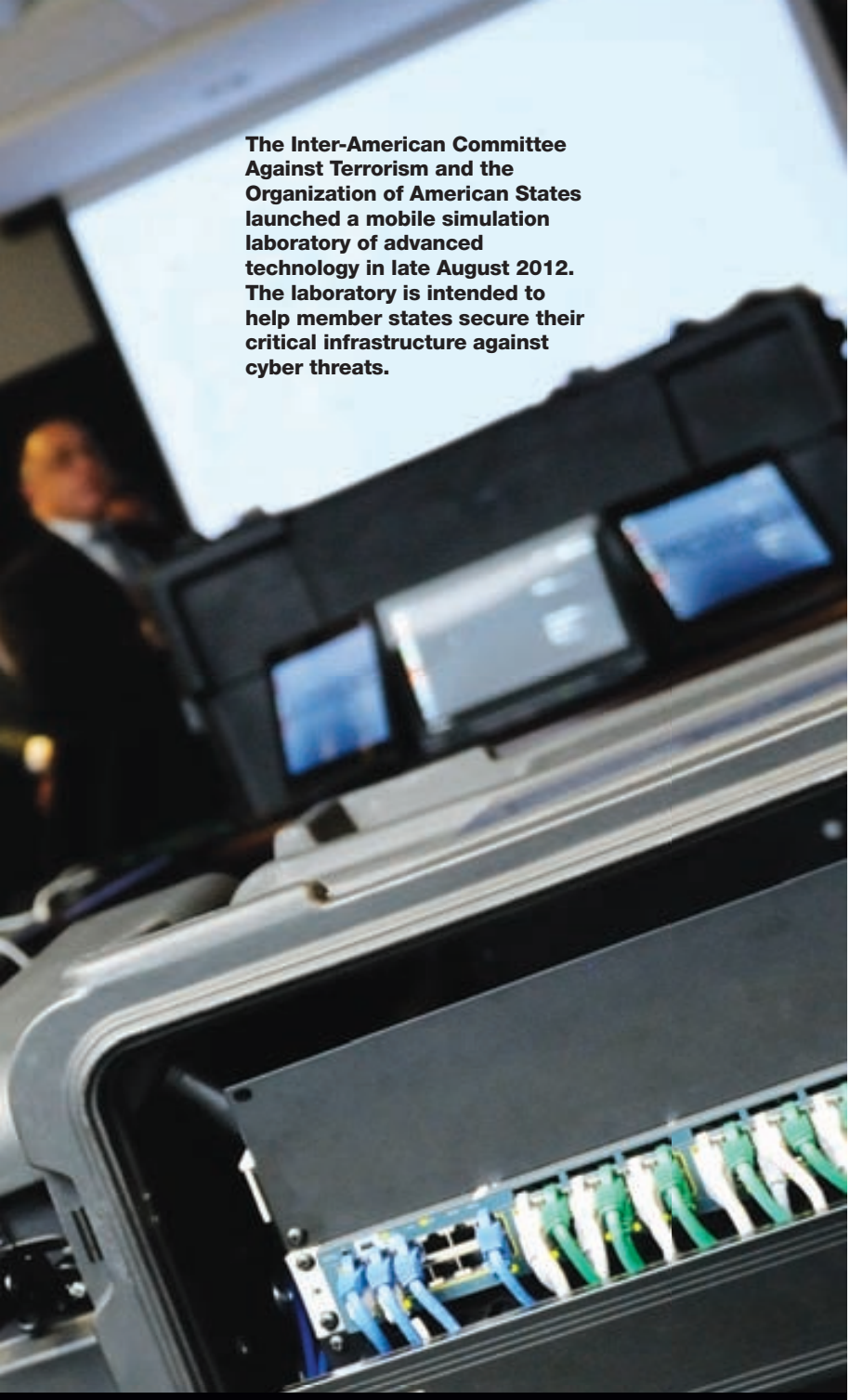
80%
of respondents say that different individuals oversee cyber and physical security at their agency.

81%
of respondents think the level of threat for cyber security will rise over the next year.

51%
of respondents think the level of threat for physical security will rise over the next year.

62%
of respondents strongly agree that it's increasingly important to coordinate cyber and physical security efforts.





The Inter-American Committee Against Terrorism and the Organization of American States launched a mobile simulation laboratory of advanced technology in late August 2012. The laboratory is intended to help member states secure their critical infrastructure against cyber threats.

12%

of respondents strongly agree that they have the resources necessary to protect against cyber security threats.

60%

of respondents say **lack of adequate funding** is the biggest challenge to security coordination.

FLICKR/ORGANIZATION OF AMERICAN STATES (OAS)

What is the top threat to your digital infrastructure and where is that threat coming from?

"The **greatest threat is to the personally identifiable data of our citizens** — the data we are the caretakers of. The source of the threat is from criminals who use the Internet to gain profit."

"Both [cyber and physical threats] are vastly underestimated in my opinion, mostly due to **lack of serious breach experiences** and 'it doesn't happen here' thinking."

"One of the greatest challenges to our security is unsuspecting internal users not realizing they are **providing passwords, account names and access** to internal and sensitive systems."

"The **biggest threat we** have comes from within."

"Lack of training of our workforce is our No. 1 threat. Folks need to be **educated on all types of threats and preventive measures** so they don't make the mistake of putting our infrastructure at risk."

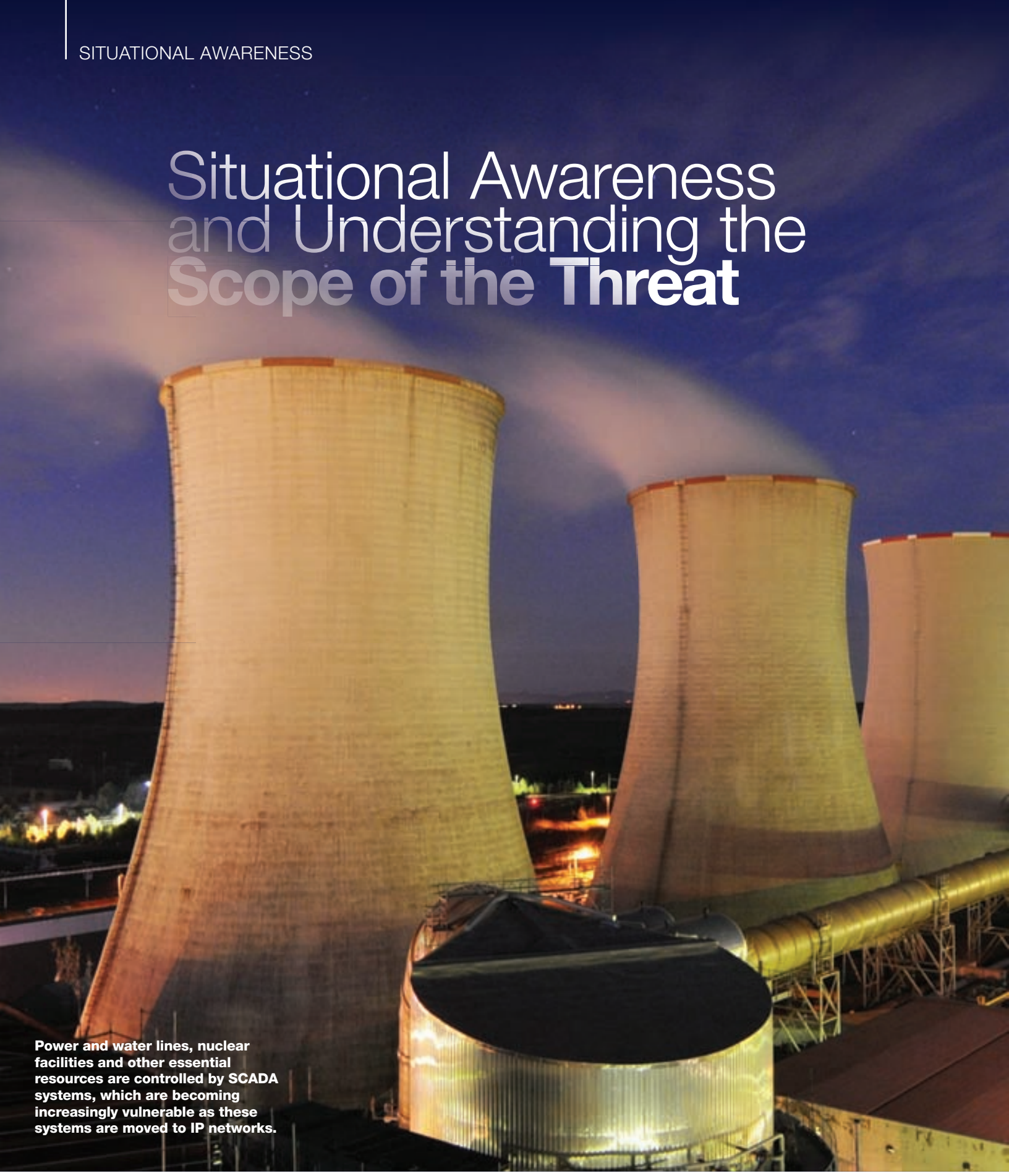
3 Steps to Better Security

Millions of attacks a day. Hackers ranging from thrill-seeking amateurs to armies of cyber experts with the full resources of a nation state. Add in political hacktivists promoting their cause célèbre and an international black market profiting from stolen financial and personal information, and it's no wonder government IT and security professionals report they're being bombarded by attacks.

What does it take to succeed in this dynamic environment? Security experts at state and local agencies and in private industry say there are no easy answers, especially in an era of tight resources and increasingly sophisticated threats. But a broad framework can help state officials evolve their strategies for protecting their valuable resources — whether they're physical or IT-related. The three-step action plan consists of awareness, prevention and prudent contingency strategies.

Will Pelgrin, chief executive officer of the Center for Internet Security, cautions agencies not to ignore the intersection between digital and physical infrastructure when performing risk assessments.

Situational Awareness and Understanding the Scope of the Threat



Power and water lines, nuclear facilities and other essential resources are controlled by SCADA systems, which are becoming increasingly vulnerable as these systems are moved to IP networks.

It's not hard to understand why state and local agencies are so attractive to today's hackers, cyber crooks and thieves. The explanation hasn't changed much from the answer early 20th-century bandit Willie Sutton reputedly provided when asked why he robbed banks. "Because that's where the money is," was supposedly his response. Whether it's true or not, this sentiment nevertheless helps explain why a mixed bag of modern burglars with widely varying degrees of professionalism and sophistication share a common interest in the critical data and resources managed by public agencies. Among the culprits:

State-Sponsored Hackers

At the top of the professionalism pyramid are state-sponsored hackers after government secrets or identifying ways to disrupt critical operations, such as municipal water systems or power grids.

"China has the largest capability to commit espionage of any country that's out there," Cyber Terrorism Analyst Morgan Wright said in a recent cyber security teleconference hosted by *Emergency Management* magazine. "The Russians are very close behind, but China has ... about 25,000 people whose job it is to patrol and monitor Internet communications."[5]

The modus operandi (MO) of state-sponsored hackers includes advanced persistent threats (APTs), which utilize the most sophisticated cyber threats, including so-called "zero-day" attacks that use never-before-seen malware to skirt existing defenses. And true to their name, APTs are persistent — launching assaults are the day jobs of the attackers, so they have the resources to devote most of their waking hours to these efforts. The ability to run undetected is another characteristic of many APTs — rather than bringing down public systems in one dramatic crash, APT malware may be designed to siphon sensitive information over time or cause incremental, hard-to-detect damage to infrastructure.

Cyber Thieves

Next on the sophistication continuum are crooks out for financial gain. As this year's Utah break-in demonstrated,[6] Social Security numbers are a big draw. Security experts say a worldwide black market exists for buying and selling personal identifiers, credit card numbers, bank account information and other keys to financial resources. The MO of these thieves includes malware that deposits keystroke loggers and rootkits, which are stealthy types of software designed to hide the existence of certain processes or programs from normal methods of detection and enable continued privileged access to a computer. Social engineering — the tricks and traps designed to get computer users to open infected email attachments or visit a compromised website — is one of the most effective strategies for delivering loggers and rootkits.

FLICKR/STEPHEN C. WEBSTER

Hacktivists are epitomized by the group Anonymous.

Hacktivists

Epitomized by Anonymous, this class of hackers is driven by political goals, including shutting down or disrupting state and local government agencies. Law enforcement agencies have been some of the most high-profile targets. Earlier this year, Anonymous claimed credit for defacing the Boston Police Department's website,[7] which led the city to temporarily take the site down. In May, hacktivists broke into the website of Florida's Lake County Sheriff's Office and released a variety of sensitive information, including the testimonies of crime victims and personal information about SWAT team members.[8] The modes of operation include many of the same tools and techniques used by APT purveyors and online thieves, redirected for political and social goals.

SHUTTERSTOCK

Ports are a physical target that can be compromised by a cyber attack.

Double-Edged Threats

Although state-sponsored cyber-terrorists, financial information thieves and hacktivists are sophisticated users of technology, their threats aren't limited to IT systems. Physical systems may also be vulnerable, with ramifications that may not only disrupt the operations of states and municipalities, but could also endanger public safety. Protecting physical resources can be just as challenging, and missteps can be deadly if they lead to destruction of the power grid, buildings, bridges, dams or seaports. Unfortunately, security officials responsible for physical security may find themselves in an especially tough fight for resources. According to the CDG survey, 50 percent of the executives said cyber security is garnering greater attention in their organizations, versus 39 percent who said that physical security is taking precedence.

But there's also a recognition that lines are blurring. Security experts say that some resources straddle the line between physical and cyber vulnerabilities. "A cyber attack on your industrial control system can produce physical effects that can result in cascading consequences," says the U.S. Department of Homeland Security's Spaulding. "Part of what we work with at state and local governments is to take a regional look at this. You have to understand the interdependencies, and look at them holistically from cyber and physical. This is not something that is just 'nice to do.' The threats and the challenges that are coming along demand this approach."[9]

For example, one physical target on the minds of a growing number of public sector security professionals today is critical infrastructure (See "Concerns Grow about Securing Critical Infrastructures" on page 16). These power and water lines, nuclear facilities and other essential resources are controlled by supervisory control and data acquisition (SCADA) systems, which are becoming vulnerable for two main reasons. First, the organizations that run SCADA systems are increasingly moving them to Internet Protocol (IP) networks. The ubiquitous networking standard handles much of the world's digital traffic, whether

The Center for Internet Security Boosts Government Cyber Security

Read story at Govtech.com:
www.govtech.com/security/The-Center-for-Internet-Security-Boosts-Government-Cybersecurity-VIDEO.html?page=1

FLICKR/PATRICK BOURY

over the public Internet or private pipelines running within enterprises. That's good news, because it gives infrastructure managers flexibility and a wealth of new tools for controlling the infrastructures and acting quickly if a natural or man-made event threatens normal operations. The bad news is that interconnectivity with public networks opens up security vulnerabilities. Security experts say sophisticated hackers throughout the world may be working to exploit openings in power systems and other critical infrastructures using cyber worms and other advanced malware. And SCADA systems aren't the only operations moving to IP networks. Video surveillance systems and alarms for doors and gates are also being supported by this ubiquitous technology.

"Understanding the cyber security concept of how these systems can be subverted or defeated is critical," says Mark Weatherford, deputy undersecretary for cyber security for the National Protection and Programs Directorate (NPPD) at the U.S. Department of Homeland Security.

Often underreported are the physical security ramifications of a cyber security breach, including the enormity of the challenge emergency management and public safety officials face if a nuclear facility or municipal water system experiences a catastrophic failure.

Will Pelgrin, chief executive officer of the Center for Internet Security, experienced firsthand how interconnected these areas become as a crisis unfolds. Pelgrin was director of New York State's Office for Technology when terrorists attacked the World Trade Center in 2001. Although most people remember the lives lost because of the physical destruction, the assaults "were also very much a cyber attack in the sense that there were consequences that were felt based upon the physical attack," Pelgrin says.[10]

> "Part of what we (DHS) work with at state and local governments is to take a regional look at this. You have to understand the interdependencies and look at them holistically from cyber and physical."
>
> — Suzanne Spaulding, Deputy Undersecretary for the National Protection and Programs Directorate, U.S. Department of Homeland Security

Pelgrin cautions agencies not to ignore the intersection between digital and physical infrastructure when performing risk assessments. For example, a risk analysis of a bridge wouldn't be complete if officials only determined what resources should be allocated to protect the structure itself and assessed only the physical and economic consequences if the bridge collapsed. "We have to ensure that the analysis includes the cyber consequences," he explains. "Because as we all know, a lot of our telecommunications run under bridges."

The consequences could snowball even further if terrorists also uncover vulnerabilities in 9-1-1 networks or even a city's traffic lights, which could thwart responses and efforts to protect the public. In addition, smaller jurisdictions and remote locations may have limited resources when it comes to staffing physical locations.

Leveling the Playing Field

It would be comforting to believe that security threats, whether cyber or physical, all originate from outside forces. Unfortunately, state and local agencies also face risks from within. Trusted employees or contractors represent security threats, whether their acts are malicious or merely careless.

But no matter whether the risks come from, outside sources or untrustworthy insiders, state and local officials have some reason for optimism. Constantly evolving security best practices and technologies are offering ways to plug vulnerabilities and protect vital public sector resources. Once security professionals understand the risks, they're ready to take the second step toward safer operations.

JESSICA MULHOLLAND

Concerns Grow about Securing Critical Infrastructures

Weatherford says DHS has developed a Cyber Security Evaluation Tool, which asks a series of questions and allows leaders to create a risk assessment of their organization.

Mark Weatherford has a unique perspective on security vulnerabilities in the nation's critical infrastructure — and it's causing him to sound an alarm, saying much more needs to be done to protect these vital resources.

As deputy undersecretary for cyber security for the National Protection and Programs Directorate (NPPD) at the U.S. Department of Homeland Security, Weatherford is on the front lines of cyber security. He guides the agency's efforts in securing IT and communications systems, and works with state and local agencies and commercial industry to improve cyber security operations. Previously, he served as California's first chief information security officer and held a senior security position for the North American Electric Reliability Corporation.

In the following interview, Weatherford discusses why critical infrastructure needs tighter security, and what resources are available to state and local governments.

Q Why is the nation's critical infrastructure seeing increased security risks?

One of the areas that I am most concerned about is the growing awareness in the black hat (hacker) community of vulnerabilities in the industrial control system environment. This environment has been around for a long time and it protects most of our critical infrastructure, including the systems and devices that open valves, open and close switches, and run generators and turbines.

The industrial control system devices themselves have typically been isolated away from the Internet, but that has changed over the last 5 to 10 years. Systems and devices that were once physically separated from the Web are now accessible to it and to wireless access. This opens up the digital vulnerabilities that we see — the nasty threats out there, including viruses and malware. The question is how to protect those critical infrastructures when the economics and the convenience of operating and managing control system devices via the Internet has become so profound.

> "The industrial control devices themselves have typically been isolated from the Internet but that has changed over the last 5 to 10 years."

Q What is the attraction of connecting these systems to IP networks?

It is much easier if I can log in remotely from home to change a switch setting on a valve rather than send somebody out to a field station or a substation 100 miles away to effect that same change. One person can manage hundreds or even thousands of devices scattered across a wide geographic area without having to touch things physically.

Q Do traditional security efforts, such as virtual private networks (VPNs), apply for control systems?

They do, but we as the owners and operators have not been as diligent about applying those kinds of controls. Most organizations are either in some process of re-evaluating how to put VPN circuits or dedicated IP-based circuits in place, or putting access control and access management policies in place.

Q What is DHS doing to help?

We have the DHS Control Systems Security Program and we also operate the Industrial Control Systems Cyber Emergency Response Team out of DHS, which is analogous to the U.S. CERT (United States Computer Emergency Readiness Team). One of the biggest advantages of the Control Systems Program is information sharing between the private sector and the government. Last year, between U.S. CERT and the Industrial Control Systems CERT, we issued over 5,200 alerts and advisories to industry and government on vulnerability-related issues. And we received [reports of] over 100,000 incidents from private sector and government organizations as well.

Q What are some of the specific resources that security professionals can draw on?

We developed a Cyber Security Evaluation Tool,[11] which is an automated tool that we provide to anybody who wants it. It's a series of questions to do a basic risk assessment of your environment. It has become a very popular application — I think we've provided it to over 1,000 different organizations.

One of the more popular and most valuable things we do is training. We have an industrial control systems training facility that is one of the best that I've seen in the world. We run a five-day training program that is open to anyone in the government or the private sector who has a need for this kind of awareness and education. We also have a one-day and a two-day program for control system security that we take on the road.

BOB RIVES

Prevention:

Proactive Approaches to Protecting Networks, Buildings — and People

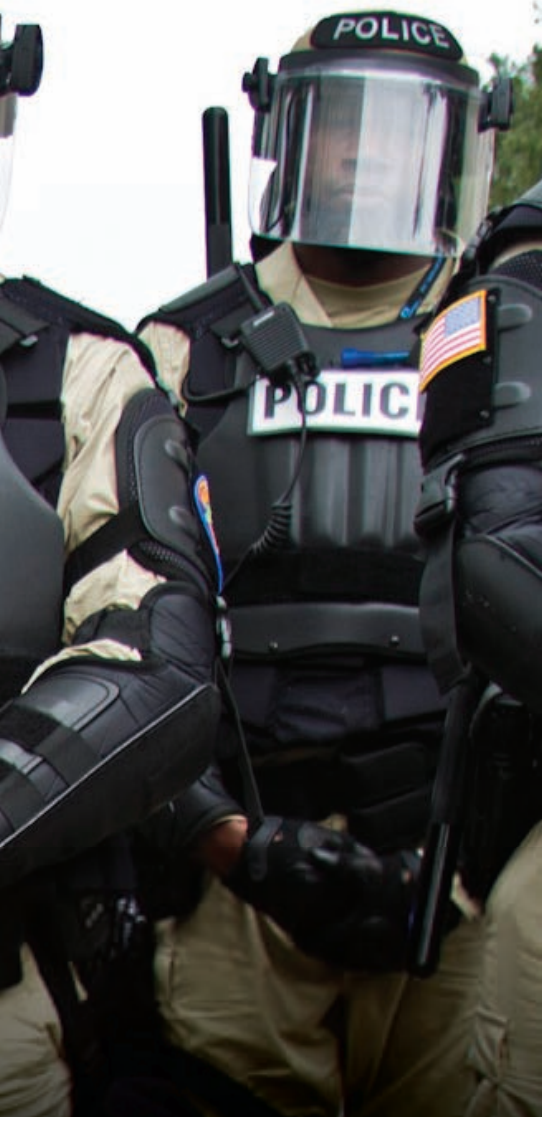
From a financial standpoint, taking proactive security measures can feel a lot like buying a life insurance policy — the upfront costs are hard to justify if life goes as planned and you never need the coverage. But spending for cyber and physical security has an extra twist — if a breach does occur, chief security officers and chief information security officers must explain why more wasn't spent to fully avert the threat.

This catch-22 has many state and local organizations performing a balancing act as threats rise and resources remain constrained. For example, 71 percent of state CIOs identified inadequate budgets as the top barrier to their overall effectiveness in the 2011 State CIO Survey conducted by the National Association of State CIOs (NASCIO).[12]

Tight budgets are leading to new priorities when it comes to security spending. "Because of resource limitations, we have to focus on areas that are the most important and apply resources there," says Chris Ipsen, chief information security officer for the state of Nevada.[13]

The CDG survey found that other IT and security professionals are also struggling with this challenge. Only 12 percent of the respondents were adamant that they had sufficient resources to effectively protect their agency against cyber security threats.

Tampa's police department augmented its on-the-ground resources during the 2012 Republican National Convention using analysis software and video cameras.



FLICKR/MOOCH CASSIDY

> "The time has come to circle the wagons and make sure that we apply whatever resources we have around our most sensitive assets."
>
> — Chris Ipsen, Chief Information Security Officer, State of Nevada

(By contrast, a higher number — 21 percent — was confident their physical security resources were sufficient.)

Fortunately, new solutions are giving public agencies more options to resolve some of the most challenging threats they face. This means creating layers of defense, starting with the basics. Anti-virus software provides what security officers like Ipsen consider "the low hanging fruit" of protection. Next in line is network security, which also takes advantage of some proven and continuing-to-evolve solutions. Filling out the list are advanced firewalls with modern protections for applications and network data packets, as well as activity monitoring solutions known as Security Information and Event Management, or SIEM. (For a full list of must-have security technologies see "New Options for Cyber Security.")

But resource constraints mean state and local officials don't have blank checks to purchase all the latest and greatest security products. Clearly there are not enough resources to make everything a top protection priority. Past practice in state and local government has been to attempt to secure the full complement of infrastructure and data equally, much like one would do with a physical asset. However, the direction organizations will have to move in is one focusing more priority on securing the most critical data with a compartmentalized strategy. This may take the form of more sophisticated and specialized security tools applied to some data and systems while others are less highly "classified." This raises important policy questions about the relative criticality of various departments, services and data. It also may require a renewed emphasis on restricting access to data and systems in a way that has historically been used only within the law enforcement community.

"The time has come to circle the wagons and make sure that we apply whatever resources we have around our most sensitive assets," Ipsen says. "We say, 'This is an area that we'll make our stand on' and employ best-of-breed solutions there, and have the best and brightest making decisions about the architectural layout of the environment."

Physical Security Safeguards

Managers responsible for physical security have their own arsenals of security weapons. These include access control systems that combine smart cards for personal identification with readers to accurately keep unauthorized persons from entering secure areas and buildings, but doing so quickly enough to avoid impeding normal operations. One tool to make such a system work is a contact-less interface that wirelessly connects cards and readers so individuals don't have to take the time to physically swipe cards.

Video surveillance systems have long acted as the heart and soul of physical security systems, but now digital varieties are gradually replacing traditional analog solutions. Digital video offers a number of benefits, including the ability to use search technology to quickly scan for specific events in a longer archive. It also supports new behavioral recognition

DAVID KIDD

Security Takes Precedence for Next-Generation 911

In the past, few states or municipalities saw a security threat in their 9-1-1 systems. After all, these self-contained resources used traditional circuit-switched voice networks to establish communications links between agencies and citizens. Hackers devoted their malware-oriented resources to bigger targets, namely the Internet and the millions of users who could potentially become vulnerable to nefarious security exploits.

But that's changing, and the risks to new 9-1-1 systems highlights how complicated the world is becoming for security professionals. Next Generation 911 systems are moving to IP-enabled infrastructures for a variety of reasons. The widely used Internet Protocol will allow emergency responders to not only receive voice calls in an emergency, but also text messages, video clips and images — anything that helps them understand the nature of the emergency and develop situational awareness. This is causing state authorities to take a purposefully cautious approach to Next Generation 911.

Some of the concerns? Someone could intentionally or unsuspectingly plug a virus-infected USB drive into a workstation at a 9-1-1 call center. The malware could quickly spread to other workstations on the network and launch a denial of service attack against the state's core emergency response infrastructure.

Physical security concerns can be just as troubling. For example, someone could walk into a 9-1-1 call center posing as a technician with the telephone company. He could go to the equipment room and upload a virus or a worm, causing the door to open up for diverting calls and terrorist attacks.

To ensure the proper protocols are in place, agencies can move to Next Generation 911 slowly, making sure they perform security assessments to identify potential cyber or physical vulnerabilities. Agencies should develop security plans that formalize security goals and compliance plans to outline how they would meet the Security for Next-Generation 9-1-1 (NG-SEC) standard developed by the National Emergency Number Association.

software that can help security guards scan for threats as they're happening.

For example, Tampa's police department augmented its on-the-ground resources during the 2012 Republican National Convention using analysis software and video cameras that kept a digital eye out for suspicious activities.[14] If the systems flagged a potential problem — such as a vehicle in a location at an unusual time of day — law enforcement officials would receive an alert and take appropriate action. Vendors of the solution say that the software can analyze videos over time to gauge normal and abnormal activities and use the insights to increase the accuracy of the warning system.

Digital video cameras also collect images to help officials develop situational awareness. To bolster security for its infrastructure and buildings and help law enforcement officials prevent crime, the city of Cleveland launched a high-speed wireless video-surveillance network in its downtown area. The effort's success encouraged the Cleveland Department of Public Safety to create the Cleveland Shared Security Surveillance (CS3) program, a public-private partnership that is expanding video surveillance throughout Cleveland. The cameras send live video feeds to a police command vehicle, the Emergency Operations Center and a dispatch center.

The resources become especially important during events that attract large numbers of citizens and visitors, such as the city's annual St. Patrick's Day Parade. "To monitor activities and provide security for all those folks is very difficult, especially on foot," says Mike McGrath, Cleveland's chief of police. "That's where video surveillance comes in. The cameras allow

officers to monitor activities in real time so they can quickly identify potential threats and respond faster and better."

On more routine days, the solution provides two fundamental benefits, says Larry Jones II, CS3 project manager. "There's better situational awareness for first responders, and that leads to increased safety — and a heightened sense of security — for our citizens and visitors."

Cleveland continues to look for new ways to use its surveillance resources, including tying them into the Computer-Aided Dispatch (CAD) system. "We want to focus on getting our video into the dispatch center where it can help police, fire and EMS as they arrive on a scene," says Jones. "We want a dispatcher to be able to say, 'Those guys just ran to the west, one's in blue, the other's in red.'"

The networking infrastructure also acts as a force multiplier. "In today's culture, where we have this flash mob mentality, for us to be able to use the video feed to observe these people in downtown Cleveland, and then relay that intelligence information to the officers on the street, is very, very important," McGrath says. "Video surveillance has definitely supplemented our workforce."[15]

Technology Evolution: IP Networks Changing the Game

Some of these technologies have been around for years, but what's new is their support for IP networks. Although this potentially may open up new risks — making the equipment vulnerable to similar malware that infects standard desktop computers, for example — safeguards are now available. When evaluating IP-based digital video systems, security managers should look for models that use security certificates to authenticate themselves. Like passwords for people, these certificates help stop hackers or terrorists looking to connect rogue cameras into an agency's IP networks to surreptitiously record surveillance videos or disrupt the flow of information from legitimate cameras.

Security administrators should also work with their IT departments to understand what upgrades to the network infrastructure may be required to support the significant increase in bandwidth-hungry video traffic that will be created with a large rollout of digital video cameras.

Embedded technologies for authentication and data security also extend to other types of systems used to lock down physical security. For example, public sector managers now have the option of choosing smart card identification systems with embedded microprocessors that use data-scrambling encryption technologies to protect the personal information stored on cards. Similarly, tamper-proof card readers can use encryption to protect authentication data or alert administrators if an unauthorized party tries to breach the system.

Additionally, agencies should secure the flow of communication between card readers and central access control systems. Encryption guards against attempts to capture information moving to and from these components.

To help determine if prospective identity card systems meet these security requirements, administrators should look for some key standards, including ISO/IEC 14443, ISO/IEC 15693 and ISO/IEC 7816. Also, watch for developments in the emerging open supervised device protocol, which is intended to secure communications between readers and access control systems.

Forging Closer Ties Between Cyber and Physical Security

The growing interconnectedness between technologies used for cyber and physical security is one

SECURITY RESOURCES

As best practices evolve to better protect public agencies, a number of organizations are publishing reference guides for cyber and physical security. They include:

- Federated Physical Access Control System Specification, from the U.S. General Services Administration
- Guidelines for Managing and Securing Mobile Devices in the Enterprise (draft), by NIST
- Federal ID Credential Security Standard, from the National Institute of Standards and Technology (NIST)
- State Cyber Security Resource Guide, from NASCIO

Dan Lohrmann heads Michigan's Cybersecurity and Infrastructure Protection organization, a bold move by the state to create an entity focused on both cyber and physical security.

COURTESY OF DAN LOHRMANN

component of a larger challenge many state and local agencies currently face. The agency staffs that manage these two areas have traditionally worked independently, separated by different professional backgrounds, expertise and cultures. In fact, only 25 percent of the executives in the CDG survey said they "strongly agree" that their agency properly coordinates cyber security and physical security efforts with other related agencies. However, 62 percent strongly agreed that in this new world of threats, it's increasingly important to coordinate cyber security and physical security efforts in order to be successful. Unfortunately, only 8 percent said they expected investments in cyber security to rise significantly over the next year, while only 6 percent predicted a significant boost in physical security resources in that period.

What's holding agencies back in their attempts to better integrate these areas? Money is one problem. When asked to name what they considered the greatest priority their agency needed to better coordinate physical and cyber security, 33 percent said they needed adequate funding. The only other priority that received a higher ranking, at 40 percent, was the need for strong commitment to the effort by senior managers.

Nevertheless, there's a growing push to formalize collaboration between cyber and physical security professionals. For federal agencies, these efforts received a boost more than a decade ago with Homeland Security Presidential Directive 12, which in part required coordination of the two security groups for identification systems. Now, security coordination is being seen as good policy throughout the public sector.

"Physical and cyber are interconnected," Spaulding says. "This is not just a 'nice to do.' The threats and the challenges that are coming at agencies demand this."[16]

Last year, Michigan made a bold move in this area, creating a new entity devoted to both physical and cyber security.[17] Named Cybersecurity and Infrastructure Protection (CIP), the new organization is headed by former state CTO Dan Lohrmann, who now holds the title of chief security officer. In the past, he also acted as Michigan's first chief information security officer.

Why make the move, which combines Michigan's state emergency management, physical security and cyber security offices? By centralizing the oversight of risk management and security issues, Michigan hopes to develop and implement a comprehensive security strategy across the entire state and improve efficiency, as *Government Technology* reported last year. "More and more systems are coming together in the physical and the cyber side," Lohrmann told *Government Technology*. "As an industry, that's happening; there's more overlap with physical and cyber security and also with critical infrastructure protection."

But differences in expertise, technology and professional cultures continue to challenge collaboration efforts. "Where I think everybody is very much playing catch-up is in fully understanding and responding to the interconnectedness of the physical and the cyber areas," says Spaulding.

What's the answer? Security experts advise agencies to tackle three key areas: technology, culture and management policies.

Even as more physical security devices connect with IP networks, technical silos continue to create barriers between physical and cyber security employees. For example, separate databases managed by each domain may hold redundant or even conflicting information for personal identification and access authorizations. Respondents to the CDG survey clearly understand the problem. As one executive noted, "It seems to me if we combined these areas of management, we would have a more efficient and effective security system. One task that should be consolidated is management of employee ID badges. They are designed to protect both physical and cyber, but each agency does their own badges, which is very inefficient."

The disparities can become critical during an emergency, for example, when first responders in the field need to connect with an agency data center to download schematics for gas mains. "Employees in one state agency manage physical security while employees in another state agency manage cyber security," says a security professional who participated in the Center for Digital Government survey.

The rise of different data formats is another information-sharing hurdle. Growing volumes of essential information now exist as so-called unstructured information — the text files, video

clips, emails and other forms that cannot be stored in traditional databases.

A variety of commercial NoSQL (not only SQL) databases are now available to manage unstructured data and work in conjunction with relational databases. The open source Apache Hadoop platform is also being used by a growing number of organizations for managing and analyzing unstructured data.

Additional technology options for merging information from physical and cyber security systems include applications that add a software layer designed to integrate separate information management systems. Some of these solutions also provide an integrated framework for governance, risk and compliance to help agencies manage diverse security systems and document adherence with regulatory requirements.

Another integration choice is Physical Security Information Management (PSIM) solutions. They provide a presentation layer that can combine information feeds from video management systems, access controllers, sensors and other security-related systems into a single view.

Efforts to integrate physical and cyber security also need to account for cultural differences among professionals, whose backgrounds run the gamut from network administration, server management and software implementation to police work, fraud investigation and intelligence. Blurring of professional boundaries mean some IT employees understand the concerns of physical security, while a law enforcement officer may have a working knowledge of computer systems, but significant gaps sometimes remain between the two.

"It's hard to find any one person who carries both the physical and cyber expertise, because they have grown up as separate disciplines," Spaulding points out. "So the challenge is to get those folks together in a room and begin to understand each other's areas well enough to know where they need to coordinate and how one impacts the other."[18]

> "The key is focusing on the outcome and getting rid of your ego — that's the biggest threat to us having a problem."
>
> — Chris Ipsen, Chief Information Security Officer, State of Nevada

Some public sector organizations are taking steps to mitigate these differences. For example, in the wake of its security breach, the state of Utah created the position of health data security ombudsman. In addition, some professionals with security responsibilities are combining formal and informal measures to coordinate their efforts with peers in their agencies. "I reach out to those people who have the authority [for physical security], and we create a unified front," says Ipsen.

Ipsen explains that he and Chris Smith, chief of Nevada's Division of Emergency Management, have been working closely to coordinate security activities. At times, this means making an effort to overcome some fundamental differences, including the different technical terms and jargon that are part of their respective disciplines. "We speak different languages, but if I can't communicate the threat in real terms, then I'm not doing my job well," Ipsen says. "I should be able to talk about APTs in lay terms. And [people in physical security] should try to learn cyber speak." Equally important is the understanding that both cyber security and emergency management professionals possess skills that are critical to the effective restoration of information systems.

Ipsen and Smith established ways to work together that include phone calls when incidents arise, regularly scheduled meetings to exchange ideas about improving security in the state, and an agreement that they will work together to overcome any impasses that come up over jurisdictional issues. "The key is focusing on the outcome and getting rid of your ego — that's the biggest threat to us having a problem," Ipsen says. "But that would be impossible if I didn't have the right person to work with."

From a management perspective, security professionals say that agency heads must balance a clear commitment to coordination and cooperation without blurring lines of responsibilities and creating confusion about areas of authority. Nevertheless, agencies may have little choice but to develop efficient ways to bridge the technical and cultural divide of physical and cyber security. "I think technology is going to continue to push us in that direction," Weatherford says.

That includes creating strong communications channels between public sector agencies and private companies, such as power companies. "We need to focus on how to take information and get it out to the communities that really need it," Pelgrin says. "Public sector agencies and private sector companies must work together to ensure that they are communicating and collaborating to be as protected as we can be. It is essential that information is available from both the private and public sectors in order to have holistic situational awareness."

New Options for Cyber Security

The varied nature of today's cyber threats mean security professionals need tools that provide safeguards on many fronts. When it is time to look beyond basic anti-virus software and network firewalls, the following solutions offer enhanced oversight and protection.

Data Encryption

What it is: Protection for information while it is stored in applications and databases, as well as when it's being sent over network links.
What it does: Scrambles data into unreadable combinations of symbols to make it useless to anyone without the proper decoders.
Bottom line: Encryption is increasing in importance as mobile devices become ubiquitous, so that lost or stolen hardware doesn't mean the release of potentially sensitive agency information. Look for applications that encrypt the entire storage drive on portable devices, including laptops, tablets, smartphones and USB drives. But encryption doesn't come without performance penalties — hardware used to encode and decode information should provide enough processing power to avoid impeding the productivity of staff members.

Deep-Packet Inspection of Network Traffic

What it is: A way to monitor the type of data traversing communications pipelines.
What it does: Analysis software peers into data packets as they move across networks to identify infected programs or sensitive information being sent to unauthorized end points.
Bottom line: IT managers should have a range of options when reacting to warnings from inspection systems. For example, known malware may be automatically blocked, while suspicious activity — someone logging into a database after hours — may be noted in an alert to a security official and entered into an event log.

Security Information and Event Management Applications

What they are: A framework for aggregating activity data from a variety of sources, including DLP and ID/IP systems.
What they do: Use statistical analyses to identify unusual or noncompliant behavior.
Bottom line: Security professionals can tap SIEM systems for a holistic view of outside threats and to monitor how staff members are interacting with internal IT resources. But experts say that SIEM isn't plug-and-play — the security staff will need time to adjust settings to reduce false alarms while not missing actual threats.

Data Loss Prevention (DLP) Systems

What they are: A safety net against security breaches caused by insiders.

What they do: Manage data downloads to endpoint devices, including mobile hardware, USB drives, DVDs and portable hard drives.

Bottom line: DLP systems help agencies enforce data-usage policies, so if the rules prohibit sensitive information from being saved to a portable storage device, the security solution will block data from passing through USB ports on agency computers. The solutions can also look for unusual activity, such as when someone moves patient medical records to a local PC or server outside of the health and human services department.

Internet Content Filters

What they are: Guards that block malware from infected websites.

What they do: Check incoming data streams for known viruses and spam or block communications from sites blacklisted by security administrators.

Bottom line: Flexibility is key when choosing systems. In addition to basic filtering settings, many solutions also allow IT managers to enter custom preferences, such as blocking all downloads during overnight hours to protect against non-business use of computer systems.

IMAGES FROM SHUTTERSTOCK

Identity Management and Access Control Systems

What they are: Safeguards against unauthorized access to agency IT resources.

What they do: Use passwords, identity cards, biometrics and other measures to identify individuals as they try to log into networks and access data and applications.

Bottom line: Identity management systems guard against intrusions by both outsiders and insiders, including employees or contractors who try to access resources they're not cleared to use. The best systems provide a central management console to make it easy for security managers to update clearances as employees change duties or leave the organization. Also important is the ability to finely tune access rights according to job function. For example, some members of the finance department may be allowed to access the accounting modules of the ERP system, but not databases that contain data about employee salaries.

Intrusion Detection and Intrusion Prevention Systems

What they are: An early-warning system for suspicious activities.

What they do: Look for communications with machines or networks known to be associated with hackers. These solutions can also analyze internal activities to flag possible breaches.

Bottom line: ID/IP solutions can either warn administrators or automatically block actions, depending on the preferences established by security officials. In addition to their real-time safeguards, these solutions also gather and report on ongoing activities to give security professionals insights into agency staff members who may not be fully complying with security policies.

Email Content Filters

What they are: A protective barrier against attacks delivered via email messages.

What they do: Identify and block malware in email messages and attachments before they can infect agency resources.

Bottom line: Email messages remain one of the biggest vulnerabilities for agencies. Sophisticated "spear phishing" attacks, which mimic messages from trusted sources, lure people to click on infected attachments or links to malevolent websites. Without effective content screening, these actions could result in rootkits, key loggers and viruses infiltrating agency IT operations. Unfortunately, because these filters work by identifying characteristics of known malware, they aren't effective against new "zero day" threats that haven't yet been fully documented by security groups.

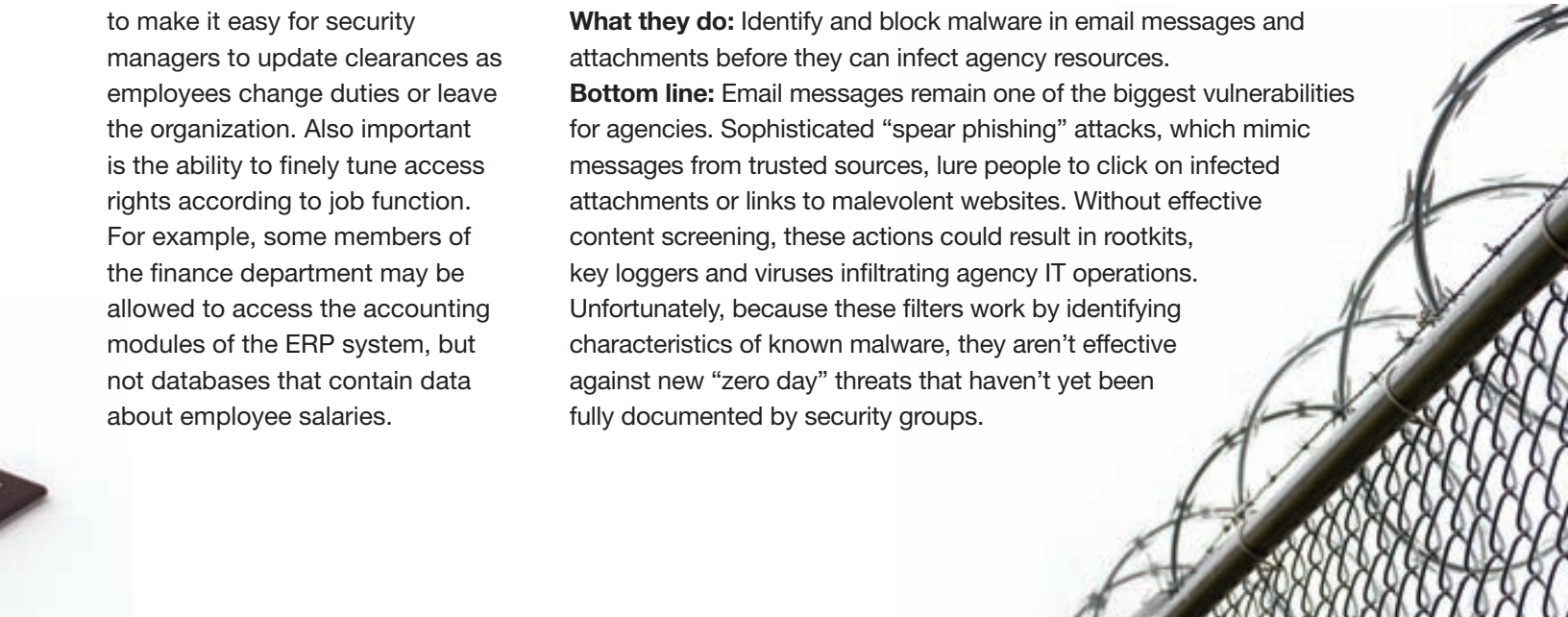


PHOTO BY DR. BYUNGHWAN LIM

Response + Recovery

How to Limit the Damage

The National Institute of Standards and Technology (NIST) in Boulder, Colo.

Despite the best efforts of security professionals and the best and brightest innovations in cyber and physical security, the uncomfortable truth is that no agency is completely safe against a security breach. A well-targeted spear phishing attack can induce even savvy email users to open a threatening attachment. Once-trusted employees with authorizations to access sensitive data may, for personal, political or financial reasons, break security policy and send the information outside the organization. Delays in completely protecting digital video systems from expanding IP networks could provide the opening a hacktivist needs to disrupt surveillance activities during a convention or major sporting event.

Security professionals who understand these realities also understand that contingency plans that spell out what to do when things go wrong are just as important as the preventive measures themselves.

Flirting with Danger

Agencies that have disaster recovery plans in place will be a step ahead of many peers. The InformationWeek 2011 Business Continuity/Disaster Recovery Survey revealed a surprising data point: Despite the obvious benefits of having a formal response plan in place when normal operations are disrupted, many organizations are winging their recovery strategies. Thirty-three percent of business technology professionals surveyed said their organizations lacked a formal business continuity/disaster recovery plan. Holdups included funding, the interdependency of systems, the complexity of putting a plan together, other higher-priority needs and/or the expense of the effort.[19]

In Nevada, cyber security and emergency management professionals are working together to address technology resiliency in a holistic manner. Their contingency strategy is designed to ensure that the state focuses on key resources and can limit the damage from security breaches so that an effective recovery is possible. He likens this philosophy to how a dirt bike rider contemplates a crash

"If you know how to fall, then you break an arm. If you don't know how to fall, you break your back. One you can recover from, and one you may not," Ipsen says. "So the key is to build a recoverable strategy."

Earlier this year, NIST released an update to its Computer Security Incident Handling Guide, which provides additional contingency plan best practices. NIST's recommendations revolve around the development of a comprehensive action plan for handling incidents. At the top of the list is an overarching statement that shows the commitment to the planning effort by senior management. In addition, a plan should make clear the incident response team has the authority to take decisive action, including confiscating or taking down equipment, according to NIST.

Start with a Plan

Stopping a security breach as it unfolds is the top priority, but security officials also need to document the incident and the agency's overall response to it. Depending on the nature of the assault, the documentation may be required if legal proceedings ensue. Additionally, clear records about the event and response will provide vital information for updating preventive measures as well as the contingency plan. NIST advises agencies to collect evidence according to procedures developed through discussions with legal and law enforcement advisors, which will help assure that the information can be admissible in court.

Need to Know

Other elements of the response plan should include details about how the incident response team will communicate its activities throughout the organization and with any appropriate outside entities. "The incident response team should discuss information sharing at length with the organization's public affairs office, legal department and management before an incident occurs, to establish policies and procedures regarding information sharing," NIST explains. "Otherwise, sensitive information regarding incidents may be provided to unauthorized parties, potentially leading to additional disruption and financial loss. The team should document all contacts and communications with outside parties for liability and evidentiary purposes."

Key to any security strategy are regular updates — NIST recommends reviews taking place a minimum of once a year — to keep responses in line with the latest vulnerabilities and best practices.

Clouds May Help

Some security and IT professionals believe cloud-based security services can help agencies respond more effectively to security breaches. Potential benefits stem first from the cloud model itself, which relieves security staffs from having to justify large capital investment for backup and continuity systems, which in some cases are rarely — if ever — used. Instead, agencies pay a set monthly fee for security and backup services, using funds from the operating budget.

A second selling point for third-party services is their ability to augment

* 33% of business technology professionals surveyed said their organizations lacked a formal business continuity/disaster recovery plan.

existing investments. An in-house security team may be prepared to respond to attacks that happen during normal business hours, while the outsourced service provider watches over the agency and responds after hours, according to the requirements outlined in the service level agreement.

> "I think that there's a value in working with the private sector because a lot of the expertise resides there. It doesn't matter if you are in the private or public sector. The attackers certainly don't care."
>
> — Chris Ipsen, Chief Information Security Officer, Nevada

Staying a Step Ahead

A multi-pronged response to security threats — spanning awareness, prevention and contingency plans — can go a long way to mitigating cyber and physical vulnerabilities. But in a fast-changing threat landscape, even the best responses must also evolve constantly. Staying a step ahead of hackers, hacktivists, nation states and untrustworthy insiders isn't easy, but some security professionals are finding strength in numbers. Many are taking advantage of federal programs, such as DHS' Industrial Control Systems Cyber Emergency Response Team or the FBI-sponsored InfraGard program, which attemps to forge relationships among security-minded government and commercial organizations.

The Multi-State Information Sharing and Analysis Center (MS-ISAC) offers resources for cyber threat prevention as well as response and recovery plans designed for state, local, territorial and tribal organizations. This includes real-time network monitoring, early cyber threat warnings and advisories.

"We've done a lot at the Multi-State ISAC to help build bridges between the physical side of the house and the cyber side of the house," says MS-ISAC founder Will Pelgrin. "We've even had exercises that use the fusion center as the point of entry to ensure that people in the center know who within their state handles cyber events. This is truly a team approach, working with trusted partners within state and local governments."

To further raise awareness about the close links between physical and cyber security, Pelgrin, as head of MS-ISAC, worked with the New York State Police and the FBI to create the Cyber Threat Intelligence Coordinating Group. The groups work together to break down the traditional jurisdictional barriers that may arise around multiple agencies. Both cyber security and physical security partnerships and working with others both within and outside the state is critically important.

Nevada's Ipsen looks to the Department of Homeland Security, the National Security Agency, the Office of the Director of National Intelligence and the SANS Institute for the latest news about new attacks and vulnerabilities. "We have an active interest in working with any and all federal agencies to gain information about threat patterns, about compromised servers, about attacks that we've seen in the wild," Ipsen says. "I also think that there's tremendous value in working with the private sector because a lot of the expertise resides there. It doesn't matter if you are in the private or public sector. The attackers certainly don't care."

THE FBI-SPONSORED INFRAGARD program attempts to forge relationships among security-minded government and commercial organizations.

ACKNOWLEDGEMENTS

Sponsors:

CenturyLink™ Government

at&t

Empowered by Innovation

NEC

hp

Acknowledgements:

ALAN JOCH specializes in technology best practices for the public sector, education and industry. His feature articles appear in *The New York Times*, *Federal Computer Week*, *Engineering, Inc.*, and other industry publications. Previously, Alan spent seven years as a senior editor for *Byte Magazine.* He is also author of the book, "How to Find Money Online: An Internet-Based Capital Guide for Entrepreneurs."

EMERGENCY MANAGEMENT

CENTER FOR DIGITAL GOVERNMENT

EMERGENCY MANAGEMENT is the only all-hazards and all-stakeholders media platform to address the entire community of senior command and policy leaderscharged to protect, prevent, respond and recover our nation from all emergencies regardless of origin. Crowned with ambitious awards, its strategic portfolio includes award-winning *Emergency Management* magazine and emergencymgmt.com, All-Hazards/All-Stakeholders Summits and Webinars, lead generation and custom media solutions.

THE CENTER FOR DIGITAL GOVERNMENT, a division of e.Republic, is a national research and advisory institute on information technology policies and best practices in state and local government. Through its diverse and dynamic programs and services, the Center provides public and private sector leaders with decision support, knowledge and opportunities to help them effectively incorporate new technologies in the 21st century.
www.centerdigitalgov.com

ENDNOTES

1. "Utah CIO Steve Fletcher Resigns, State Promises Security Reforms." *Public CIO*, May 15, 2012, www.govtech.com/pcio/Utah-CIO-Steve-Fletcher-Resigns-State-Promises-Security-Reforms.html
2. Alan Joch interview with Christopher Ipsen, August 7, 2012
3. Center for Digital Government research survey
4. Alan Joch interview with Mark Weatherford and Suzanne Spaulding, August 22, 2012
5. "When Worlds Collide: The Converging Threats to Governments' Physical and Cyber Infrastructure." *Emergency Management* Cybersecurity Teleconference, July 11, 2012, http://forms.erepublic.com/EV-1061?elq=652cb19c746d4eb8bb67673ef84dce9delqCampaignId=1350
6. "Utah CIO Steve Fletcher Resigns, State Promises Security Reforms." *Public CIO*, May 15, 2012, www.govtech.com/pcio/Utah-CIO-Steve-Fletcher-Resigns-State-Promises-Security-Reforms.html
7. "Hackers Deface Boston Police Website," Boston.com, http://articles.boston.com/2012-02-03/news/31022314_1_police-department-police-handling-law-enforcement-agencies
8. "Lake sheriff hackers reveal flaws in police computers," Orlando Sentinel, May 5, 2012, http://articles.orlandosentinel.com/2012-05-05/news/os-hacking-site-lake-sheriffs-office-20120505_1_anti-sec-cyber-security-anti-security
9. Alan Joch interview with Mark Weatherford and Suzanne Spaulding, August 22, 2012
10. Alan Joch interview with Will Pelgrin, August 8, 2012
11. Control Systems Security Program, United States Computer Emergency Readiness Team, www.us-cert.gov/control_systems/csetdownload.html
12. "A New C4 Agenda: Perspectives and Trends from State Government IT Leaders," The 2011 State CIO Survey, NASCIO, October 2011, www.nascio.org/publications/documents/2011%20State%20CIO%20Survey%20final.pdf
13. Alan Joch interview with Christopher Ipsen, August 7, 2012
14. "GOP convention will use 'behavior recognition' software on video surveillance cameras in Tampa," Government Security News, August 20, 2011, www.gsnmagazine.com/node/27048?c=video_surveillance_cctv
15. "Safety in Sight: Video Surveillance Protects Cleveland," www.motorola.com/web/Business/_Documents/_staticfiles/Cleveland_Motorola_Video_Surveillance_Case_Study.pdf
16. Alan Joch interview with Mark Weatherford and Suzanne Spaulding, August 22, 2012
17. "Michigan Merges Physical and Cyber-Security Offices," www.govtech.com/security/Michigan-Merges-Physical-and-Cyber-Security-Offices.html
18. Alan Joch interview with Mark Weatherford and Suzanne Spaulding, August 22, 2012
19. "Research: BC/DR and the Cloud," *InformationWeek*, November 11, 2011, http://reports.informationweek.com/abstract/2/8561/business-continuity/research-bc-dr-and-the-cloud.html

We can protect what matters. Together.

The cloud, mobile technologies, and social networking offer new opportunities for governments—but also create some of your biggest security challenges. HP's proven and innovative security solutions can help you manage risk, be compliant, and maximize your investments. We help you build security in and make it intelligent to protect the information that matters.

hp.com/go/cybersecurity

Start Solving your Agency's Puzzle with CenturyLink Government

Offering a comprehensive solution of network and managed services

Unified Communications • Security Solutions • Cloud Services

visit us online at: www.centurylink.com/government

CenturyLink® Government