

SEARCH THE
 SITE


[Advanced
Search](#)

 ALSO
 ONLINE

[Events
Calendar](#)
[Letters](#)
[Archive](#)
[Online](#)
[Archive](#)
[Print Archive](#)
[Milt Zall](#)
[Columns](#)
[Special](#)
[Reports](#)

 NEWS BY
 TOPIC

[Accessibility](#)
[CIOs](#)
[Columns](#)
[Defense](#)
[E-](#)
[Government](#)
[Funding](#)
[Homeland](#)
[Security](#)
[Industry](#)
[Intergovernmental](#)
[Law](#)
[Enforcement](#)
[Management](#)
[Policy](#)
[Privacy](#)
[Procurement](#)
[Program](#)
Federal Computer Week

Testing the tech

Disaster simulations count on successes and failures for the best results

 BY [Heather Hayes](#)
 Aug. 25, 2003

As they face purposeful catastrophes rather than those occurring naturally or accidentally, emergency management officials expect that information technology will play a key role in helping them respond to disasters and save lives.

But even though cutting-edge technologies promise to instantly detect a chemical that's been released on a city street, for example, or provide critical information simultaneously to decision-makers in different locations, there are no guarantees of how these technologies will perform during a real terrorist attack.

As a result, emergency managers are conducting exercises nationwide with an increasing sense of urgency and a willingness to put technology

 Printing? Use this
[version.](#)
[Email](#) this to a
 friend.

RELATED LINKS

 Sidebar: [Federal agency finds local planning helps a seller's market](#)

 Sidebar: [Tips for exercise planners](#)

 Sidebar: [An immersion excursion](#)

["HHS center put to test by terrorist exercise"](#) [Federal Computer Week, May 26, 2003]

["Collaborative tool aids terror exercise"](#) [Federal Computer Week, May 13, 2003]

["Models of](#)

Sponsored By:







[Management Records Management Seat Management Security State & Local Technology Telecom Training Workforce](#)

READER SERVICE

[Advertise](#)
[Contact us](#)
[Editorial](#)
[Calendars](#)
[E-mail](#)
[Newsletters](#)
[Linking to us](#)
[Links](#)
[Disclaimer](#)
[Online](#)
[Permission](#)
[Privacy Policy](#)
[Site Map](#)
[Subscriptions](#)

[Site Problems?](#)

VENDOR SOLUTIONS

[PC Mall](#)
[Catalog](#)
[IBM White Paper](#)
[HQ SSG](#)
[Acquisitions Directorate](#)
[Adaptec](#)
[White Paper](#)
[IT as a Utility](#)
[HP White Paper](#)

through some tough paces. The exercises include everything from TopOff2, a high-profile national springtime event that tested the ability of multiple jurisdictions to respond to simulated biological and nuclear attacks, to more focused local and regional exercises, such as San Diego's recent Shadow Bowl.

[mayhem](#) [Federal Computer Week, Sept. 30, 2002]

"A lot of things sound good in theory and there are all kinds of claims made about what technologies are capable of, but until you actually put them in the context of procedures and human response, you just don't know how they'll perform," said Chad Foster, a policy analyst with the Council of State Governments. "And you definitely don't want to find out about bugs or issues while you're in the midst of a disaster."

Making a Choice

Despite issues of interoperability among information systems and the lack of a good handheld device that can immediately distinguish between, say, anthrax and baby powder, emergency management personnel and exercise planners do have a wealth of state-of-the-art technologies at their disposal.

Among the choices available now are wireless sensors that can detect the presence of chemical, biological and radiological materials; plume dispersion models; rapid data search and knowledge management tools; Web-based, unified command and control and situational awareness systems; and video surveillance equipment programmed to alert officials to specific activities.

However, testing a technology during a homeland security exercise is not as simple as handing out gadgets to emergency workers and turning them loose.

Technology needs to be included in the planning stage, according to Jerry Koenig, exercise coordinator for the Alaska Division of Homeland Security, and planning is critical to success.

"You've got to have a plan to exercise against, with clear objectives," he said. "Otherwise, it will all be just controlled chaos. Then the technologies you choose have to meet your needs and support your objectives."

[GSA](#)
[CONNECTIONS](#)
[SoftwareAG](#)
[White Paper](#)
[ECS III](#)

During the recent Northern Edge exercise, conducted annually by the Defense Department and Alaska officials, the state was testing, among other things, the federal response to a local request for assistance, with a primary objective of improving communications among agencies.

Two technologies were tested: the new Alaska Land Mobile Radio System, which promises to provide seamless communications across all levels of government; and Open Text Corp.'s FirstClass conference room-based communications software.

Having clear objectives also makes it easier to make post-test fixes to any problems that arise. Koenig noted that during Northern Edge, some workers had difficulty operating the radios. But exercise officials quickly surmised that the issue had more to do with training than with the equipment itself.

"We found that a lot of people would walk into the initial training class, see the radio and think, 'I've operated radios forever' and not listen," he said. "They'd later come back with the radio that they said didn't work. We'd give them an identical one and then take the opportunity to give them a bit more training. When that happened, those people experienced no more problems during the exercise."

High-Tech Tools

The latest and greatest technologies can not only enable emergency management personnel to reduce the effects of a terrorist attack, they can also help employees be more prepared for the possibility.

Today's simulators, modeling programs and Web-based incident management programs are just some of the available technologies that let exercise planners overcome logistical challenges and create truly realistic scenarios.

Florida officials, for example, used modeling and geographic information systems in an exercise this spring that tested state and local response to a dirty bomb scenario in the port of Miami.

"Traditionally, you would try to estimate what the plume

would look like and maybe generate a graphic," said Craig Fugate, director of Florida's Division of Emergency Management. "But we were actually taking data about dispersal, wind speed and weather, putting it into the model and then running that model to project what the event would look like. We could then use that to drive the exercise."

During TopOff2, a national weapons of mass destruction exercise series, planners used a Web-based incident management application called E Team from E Team Inc. The application helped coordinate the efforts and input of personnel and officials nationwide. Homeland Security Secretary Tom Ridge even used the system to monitor the situation from his office in Washington, D.C.

E Team has already proved itself in responding to an actual event. It was used in the aftermath of the Sept. 11, 2001, terrorist attacks and the Washington, D.C., area sniper shootings, as well as numerous natural disasters.

The program also helps exercise planners deal with getting exceptionally busy people to the emergency operations center at the same time. Without leaving their offices, participants can log on to E Team, view situational summaries in real time and receive resource requests and update notifications via e-mail. As a result, exercising can take place without quite as much strain on schedules and resources.

"Even if someone's on vacation, they can check in, respond to a notification and then go back to the pool," said Eric Kant, professional services manager for E Team. "You really can't put a value on that."

Achieving Success

Still, exercise planners often make the mistake of listing too many objectives or setting out to test too many technologies. That approach can cloud their ability to distinguish between a real problem with a procedure or technology and what's known as an exercise anomaly — the natural result of human error and too much activity.

For San Diego's Shadow Bowl exercise — a unique approach that involved testing procedures and technologies amid efforts to secure January's Super Bowl — planners had access to a variety of the latest and

greatest equipment, all donated for the two-day event by businesses and research organizations. They included car-counting sensors, water supply-contaminant sensors, people-tracking devices, surveillance systems, wireless communications, plume modeling applications, and a telecommunications disaster recovery system.

"It was an opportunity to do a real-time exercise next to a real-time event with real-live threats," said Bob Davis, a San Diego police officer and technical director of the exercise.

The exercise ultimately achieved its objectives of helping secure the Super Bowl and showcasing the value and practicality of cutting-edge technologies. Unfortunately, San Diego officials will not be able to buy any of the technologies for use in an actual terrorist attack, thanks to a budget crisis that has gripped the city and the state of California.

Some experts believe the golden rule for testing technology during scenario-based exercises is "practice like you play." Shadow Bowl broke that rule. By using technologies that are not available in the real world, experts say, planners run the risk of teaching personnel the wrong actions or the wrong conclusions, either of which could be detrimental in the event of a real incident.

R. David Paulison, director of the Preparedness Division at the Federal Emergency Management Agency, said new technologies should be fully evaluated and tested in a laboratory or during tabletop or limited departmental drills before being used in a scenario-based exercise.

"You want only those technologies that are fully available to the personnel," he said. "It doesn't do any good to pretend-practice something that isn't available the day of the exercise or truly practice something that won't be available on the day of a real event."

Planners also should avoid choosing technologies based on promise or hype. Instead, Fugate suggests using what he calls the "so what?" test. A new technology can access numerous resources simultaneously in real time and produce 3-D graphics. But is it just more noise and pretty pictures, or will it help key personnel make decisions? If the answer to the latter question is no, then don't choose

that technology.

"What's going to help me in a timely fashion to get that piece of information during a chemical attack that helps me decide not to order an evacuation but to tell people to shelter in place because if they evacuate they'll head straight into a toxic cloud?" he said.

"The technologies that are used shouldn't merely dazzle," he added. "They need to be capable of actually improving the outcome of the event, whether that's responding more quickly to the incident or decreasing the number of casualties."

Hayes is a freelance writer based in Stuarts Draft, Va. She can be reached at hbhayes@cfw.com.



FCW.COM is a product of FCW Media Group, a division of 101communications LLC