Katrina’s Hard Lessons

With new tech systems in place, Red Cross is better prepared to cope with disasters

A YEAR AFTER THE DEADLIEST U.S. hurricane in nearly eight decades, leaving an estimated 1,600 to 1,900 people dead in its wake, the American Red Cross says it has implemented new IT systems to respond to disasters of such gargantuan scale. They include an emergency assistance call center to handle up to 100,000 cases a day; a centralized national shelter system that gives governments, relief agencies, and others needed information to plan and manage shelters and evacuations; and a disaster welfare information system to inform families of the whereabouts of their loved ones.

Many of the organization’s 600-member IT operations worked 12-hour days, six days a week, to get the systems ready for the 2006 hurricane season. With a $5 billion budget and 35,000 paid employees, the American Red Cross spends $200 million a year on IT.

Legacy systems supported Red Cross services for previous disasters, including the four hurricanes that struck Florida in 2004. In that period, the Red Cross assisted some 75,000 families and 156,000 people, handing out $35 million in aid. But those systems proved no match for Katrina. During that storm, the Red Cross assisted 1.3 million families and 4 million individuals, dispersing $2 billion in aid. It responded to the 2004 hurricanes with about 1,500 volunteers and staffers. With Katrina, the number of workers soared to 200,000.

The seat-of-pants solutions devised a year ago have become the foundation of some of the new systems being implemented today. Take, for instance, the call center. The Red Cross has relied on a virtual call center, in which a distributor routes calls to trained volunteers, some working in their living rooms, to provide disaster survivors with assistance. A typical call could take 45 minutes.

But the number of victims from Katrina overwhelmed that system. In the storm’s aftermath, the Red Cross received a million calls a day from victims, but could handle no more than 3% of them at a time. “We can’t operate that way,” Red Cross CIO Steve Cooper says. “We can’t say to someone in desperate need of service, ‘Where are you, we’ll call you back,’ or put that person on hold.”

Recognizing that the legacy call center staffed by volunteers can’t handle a Katrina-like catastrophe, the Red Cross has retained Verizon to run a professionally managed call center. The plan calls for professional call center personnel to either resolve a problem in five to 10 minutes, or elevate it to the next level. The new call center, which is ready for deployment, will be used only for the biggest disasters. It can handle 1 million calls in 10 days and another 2 million calls in an additional five days.

SCALE UP

Staffing remains a challenge. A disaster like Katrina would require 10,000 call agents to staff 4,000 seats around the clock to handle 100,000 cases a day. Cooper is asking businesses to see if their employees would volunteer to be trained as caseworkers for the worst-case-scenario storms. To link these workers with the call center, the Red Cross would ask its telecom providers—including AT&T, Sprint Nextel, and Verizon—to create a virtual network of networks. Cooper sees that type of network allowing the center to handle 10 million cases.

Because of the massive geographic scope of Katrina, another lesson learned was the need to centralize information about shel-
ter availability, evacuation routes, and survivor whereabouts. Such information customarily had been stored and analyzed in a patchwork of systems operated by local, state, and federal government agencies with little interconnectivity. Based on integration technology called Tapestry from VisionLink, the Red Cross and the federal government jointly created the National Shelter System, which uses the Internet to give government agencies, relief organizations, and others access to information they need to plan and manage shelters and evacuees. The system identifies some 40,000 facilities that can be used as shelters, as well as the network of roads and transportation networks leading to and from them.

Emergency and disaster relief personnel use its mapping tools to track in real time where evacuees are headed. It’s not always obvious. Planners had expected many of the Gulf Coast Katrina evacuees to head north, but most went east and west. The Red Cross operated 1,100 shelters in 27 states and them to shelters "with a clarity that was never possible before," says W. Michael Brackney, American Red Cross' manager of client services program development.

PLAN AHEAD
Another change brought on by Katrina is to provide more than 800 local Red Cross chapters with software to let them track client assistance and document the services the agency provides to victims. In effect, information is predeployed to locations where a disaster could occur.

The Red Cross also has established the "safe and well" Web site that lets loved ones search for the whereabouts of family members. As a security measure, those conducting the search must provide known information about the missing relative or friend, such as a phone number or street address.

The Red Cross has documented the best practices it learned from Katrina in its Extreme Mobilization Playbook that it will share with local, state, and federal governmental authorities and businesses. Cooper also is soliciting ideas from the IT community for the best and most cost-effective ways to deploy rugged, mobile application servers, laptops, and other technologies at shelters to provide clients with services. He's seeking a better understanding of how to quickly link shelters to the Internet and Red Cross networks, and to exploit technologies such as Wi-Fi and wikis. Cooper is looking for secure technologies and processes to quickly distribute millions upon millions of dollars to disaster victims in need, yet prevent fraud.

Specifically from CIOs, Cooper wants to learn what they liked and disliked about technologies they've tried. "If somebody else already has experience," he says, "I want the benefit of their experience on behalf of the Red Cross and literally on behalf of the American public."

— ERIC CHABROW (echabrow@cmp.com)

Get InformationWeek the way you want it at: informationweek.com/myiwk

VPN Danger Zone
Despite security tools, strong authentication is needed for remote access

YOUR SECURE SOCKETS
Layer VPN still may not be as secure as you think, especially if your users don't always access the network via corporate-issue laptops. Once they jump on an outside machine to browse the Web or check e-mail, SSL VPN users can leave behind sensitive data and are vulnerable to man-in-the-middle attacks and keystroke loggers. An infected kiosk can infect your network, too. So even though they may be more convenient than their IPsec counterparts—SSL can be used by browsers anywhere, without client software—these VPNs can backfire if you're not careful in how you deploy them.

SSL VPNs are popular among en-