Hands Across the IT Borders

Darby Patterson | April 16, 2002

As New York continued to dig through the rubble of the World Trade Center, governments at all levels looked for lessons that might be salvaged from the nation's tragedy. How might other jurisdictions build the electronic framework to respond to the demands of a changed America? The Center for Digital Government, the knowledge-management and research division of e.Republic, and Government Technology magazine hosted a homeland security teleconference with a panel of local, state and federal officials weeks after the attacks. Reflecting the intense interest in government's response, hundreds of attendees listened in and asked questions.

Panelists were quick to point out that, although America's focus and concerns have changed since Sept. 11, much of the technology used to respond to the emergency was already in place. "Like a lot of other people, we found out how good our Y2K plans and contingency planning were," said the OMB's Tony Frater, adding that agencies are being asked to look at places where weaknesses were found and correct those conditions. "One of the critical things we need to do is be integrated in our response to things."

The Government Information Security Reform Act, passed in 2000, should help governments do that, according to Frater. Under the legislation, federal agencies were required to report to the OMB and Congress about the security of their systems. Along with analyzing those reports, Frater said there would also be a focus on what Tom Ridge, director of the U.S. Office of Homeland Security, referred to as "data integration."

"We are thinking in terms of both geo-spatial data and various decision support systems, knowledge-management systems and how we can distribute our decision-making capabilities to ensure we have the best information available," he said. "I know we've gotten requests from a number of state and local governments about how we can do a better job of integrating federal, state and local government information assets."

Coming from the federal sector, this kind of outreach to other government entities comes as a welcome sign to state officials who have advocated for more systems integration and standards. Utah is a state that's been ahead of the curve thanks, in part, to a governor who has been a strong advocate for digital government. In addition, the state is playing host to the 2002 Winter Olympics, an event that poses as many threats as it does economic benefits.

According to Chief Privacy Officer Al Sherwood, the state budgeted an additional $40 million in security costs. Data sharing with the FBI has increased, he explained, and one project is under way to link the state's GIS data layers to the Olympic command centers.

"Data integration becomes difficult at the state level, unless it's going on at the federal level as well," he said. "FirstGov and other initiatives are great opportunities to do more on that."

Sherwood said GIS data on bridges, power plants, refineries, storage tanks, hospitals and other sensitive facilities must be available for planning and operations. "The area we need more coordination in is the coordination of GIS information," he said. "What we need to do is make this information available to our command centers." And some GIS data has been removed from the Web, he added, to avoid making it too easy for terrorists to find targets. In preparation for the Winter Games, local law enforcement is cross training with the FBI, and crime analysts have access to one another's databases. Sherwood added that Utah had its Web site hacked and defaced prior to Sept. 11, raising awareness and inspiring the state to launch additional security measures.

Sherwood was appointed to the privacy post in the summer of 2001. He said that when he first embarked on his mission under the direction of CIO Phillip Windley, his focus was on creating effective privacy policies and protections. "How I spend my days now is a whole lot different than

before Sept. 11," Sherwood said, admitting the privacy focus has shifted. "I spend a great deal of my time talking about security."

Utah has implemented a firewall initiative, installed intrusion detection systems and, by order of Gov. Mike Leavitt, launched a Homeland Security Task Force. Although the state had an early start in the security arena, Sherwood admitted the September events had an immediate impact. "It really sped up the deployment of plans we already had in place," he observed.

Near the hub of terrorist activity, West Virginia was also early to adopt a security focus. The priority came with the January 2001 appointment of chief technology officer Keith Comstock. "A lot of my background has been supporting federal clients, particularly in the Department of Defense, and so I came with a certain mindset about protecting data," he said in an earlier interview with the Center for Digital Government. "One of the things I did when I came in here was to hire a security officer, and at that time I got a lot of strange looks. Now, I'm having to re-examine where I was - I wasn't being strict enough."

Since Sept. 11, Gov. Bob Wise approved crisis funding for security enhancements and a liaison with the federal Office of Homeland Security. West Virginia state employee ID cards have been reissued and National Guard troops have been deployed to guard airports. Comstock said the state did a security assessment early last year and found that 89 percent of 5,000 passwords tested were cracked in five minutes or less, and 30 percent of desktop machines contained unauthorized software. Those conditions were quickly corrected. [Query to Production: Can you represent this graphically?]

Comstock said the state's top 10 security priorities include business continuity planning, screening of personnel and issuing security clearances, activating intrusion detection systems, increasing the use of biometrics, recruiting security officers and other priorities. Comstock said simple directives, such as making sure doors are locked and server racks are secure, need to be enforced. "There are no easy answers," he said. "You need money, leadership and political capital to make the necessary changes."

The state's information security officer, Steven Lee, speculated that electronic government initiatives will move forward, rather than be stalled as states seek to respond to new demands. "I do see that there is going to be a complete buttoning down of systems," he said. Nonetheless, he expects a renewed demand for e-government services. "I don't want to speak for the governor, but the promise he's made to the citizens is to create an e-government initiative that brings government closer to the people through technology, and in doing so, make absolutely sure there is security," Lee said.

Planning Ahead

While other state and local governments looked at homeland security from a mostly theoretical platform, the city of New York was dealing with reality. Avi Duvdevani, acting CIO for the city, agreed that Y2K planning provided critical support throughout the crisis. A four-step plan for business continuity had already been designed and tested.

The plan, which covered facilities, PCs and servers, labor and network connections, was used occasionally prior to Sept. 11 for fires and electrical outages, according to Duvdevani. When the Twin Towers fell, the plan continued to work even though the scale of the disaster was unprecedented.

"One of the most devastating consequences from the technology perspective was the impact on the city's telecommunication infrastructure in the city center area," Duvdevani said. Ironically, the attacks happened just days after Duvdevani, a 20-year veteran of city-service, was named acting CIO. After the attacks, he said, police headquarters, City Hall and many other buildings were forced into "total communication darkness" when Verizon's central office was impacted by the collapse of building seven of the World Trade Center, the building that housed the city's emergency-management command center.

The communications shutdown hit more than 50,000
phones and thousands of data terminals that controlled city operations. "In the wake of all that carnage, my agency was shouldered with the responsibility of restoring communication as quickly as possible to high priority buildings," he reported. While Verizon focused on enabling emergency services, Duvdevani's office looked for options and found some in place.

The city's Mutual Assistance and Restoration Consortium was a group formed in the early 1990s to provide voice and data alternatives in case of critical data disruptions. Under the agreement, broadband telecommunications providers were required to offer mutual assistance in critical circumstances. In the immediate aftermath of the attacks, appropriate carriers were called upon to bring key sites back up. "We restored City Hall and the Municipal Building in three days with alternative fiber, wireless and other esoteric solutions," said Duvdevani. One of the most unique solutions included the city going to court to get permission for a bankrupt company to provide Internet wireless devices during the disaster recovery.

GIS in the Spotlight

Underscoring the important role of GIS in disaster recovery, Al Leidner, New York City's GIS manager, supported the restoration of services. Duvdevani said police helicopters took professional photographers aloft, where they took aerial shots of the destruction. The photography was overlaid on utility, water and power outages.

"The task ahead of us now is to strategically develop an approach [to] how we can leverage this investment we have made into a more strategic solution," Duvdevani said, adding that the city had already planned redundancies into its system. Nonetheless, like most government entities, he admitted New York agencies often resisted internal communication. The September disaster highlighted just how important cross-agency communication is in disaster response.

Protecting E-Government

Although the city had an aggressive security stance and had implemented intrusion detection, Duvdevani added that his first move after the attacks was to take the city's site down. He was concerned that too much information, such as traffic patterns and detailed maps of city sites, might aid the terrorists in some way.

There was consensus among call participants that the events of Sept. 11 did not sound the death knell for electronic government. On the contrary, they speculated that access to information and services from government will become increasingly important. "There will be no slow down in our e-government initiative," Duvdevani said. "In fact, it's accelerated." He suggested alternative technologies, such as increased deployment of wireless services, will be employed to create even more avenues of communication.

Interagency and intergovernmental cooperation are key to this vision of the digital future. According to the OMB's Frater, the appointment of Mark Forman to the federal e-government office sets a national IT agenda that includes enterprise systems. The OMB's focus is on government-to-government data integration. "We started scrubbing the base and looking at agency IT requirements. We saw the same type of requests coming from multiple agencies," Frater said. "Now, we are thinking a little more broadly

and thinking this is the same system we're using in 10 different agencies. Let's build it once and replicate it and that frees up other money that we can use in new ways."

This new federal mindset includes state and local governments. Frater said many non-federal entities have contacted his agency for guidance and to offer assistance. Consequently, the OMB reached out to the National Association of State Chief Information Officers, the National Association of Counties and other state and local groups, as well as GIS associations. The OMB will focus on several data integration initiatives with state and local governments, Frater said, including GIS, vital information from the Social Security Administration, disaster information and tax and wage reporting.

In addition, Director of Homeland Security Tom Ridge has announced his focus on coordination of activities and agencies. "It is critical to him to have enterprise tools to make data more effective, and the president has also cited working with state and local government as one of his main priorities," Frater observed.

Conversations with leaders in digital government support the observations made by panel participants. Security has been a constant concern in the deployment of information systems. Enterprise-wide thinking and interagency communication have long been regarded as necessary elements in electronic government.

Digital signatures, shared PKI, systems integration and intergovernmental collaboration are being discussed at the highest levels. Federal officials who now acknowledge the interdependency of information systems needed to create true national security are inviting state government leaders to the table. Local governments, long relegated to the outfield of technology, have suddenly become valued team members. From the challenging aftermath of Sept. 11 emerges an opportunity to develop truly integrated electronic government without boundaries.