

Microsoft **Homeland Security**



Good Connections

Microsoft technology links justice, public safety
and health communities for a unified response.

MICROSOFT

Repeatable collaboration solutions help keep America safe.

Government agencies must work together as never before to protect citizens from terrorist threats. Public health and safety organizations need to collaborate across jurisdictions to deter attacks, and they must plan jointly to respond to attacks that do occur.

Federal, state and local agencies throughout the nation rely on Microsoft and its industry partners for interoperable solutions to strengthen homeland security. In Missouri, for example, public safety agencies collaborate through a Web portal created by Convergence Communications, based on Microsoft SharePoint technology. In Alabama, the Law Enforcement Tactical System uses Microsoft BizTalk Server to give police access to data maintained by other law enforcement agencies statewide.

Public safety officials from 39 jurisdictions in King County, Wash., use a system built on Microsoft SharePoint Portal Server and Microsoft Live Meeting Server to hold online planning sessions, complete with slides, documents, videos and other tools. The Michigan Health Alert Network — supported by SharePoint Portal Server and Microsoft Active Directory, and based on software from Microsoft industry partner Virtual Alert — links 180 hospitals, allowing any participant who detects signs of a possible bioweapon attack to broadcast an alert to all the others. And when dangerous incidents occur in Houston, the public school system quickly contacts parents via e-mail, phone or pager using a system built by Microsoft partner Dialogic Communications Corp.

On the federal level, Microsoft and several partners helped the Department of Homeland Security (DHS) develop the Joint Regional Information Exchange System (JRIES),

a system for sharing homeland security information among officials in the 50 states and five U.S. territories.

Many DHS funding programs promote development of innovative technology solutions, and they encourage agencies from different jurisdictions to work together. States and communities may tap additional DHS sources, such as the Urban Area Security Initiative Grants program, to fund technology implementations for planning and preparedness.

“Along with an increase in federal homeland security funding, there is accelerated growth in statewide spending on these kinds of projects,” said Tom Richey, Microsoft’s director of homeland security. “It’s not just happening in the law enforcement community, either. The health community is connecting its constituencies to each other, and in turn to the local public officials for purposes of sharing information, response and recovery, alerts, and warnings.”

Chief information officers at the state, county and city level can play a vital role in implementing interoperable homeland security solutions. With their broad perspective, they help public health and safety stakeholders leverage existing applications and infrastructure for new uses. “The CIO can show homeland security planners solutions that have been productive in other areas of government and explain how these solutions will make their own operations more efficient,” said Mike Byrne, Microsoft’s director of justice and public safety.

Keeping Americans safe means building an intelligent, robust and highly integrated homeland security infrastructure. Microsoft and its industry partners are delivering repeatable solutions that enable governments to make the right connections.

Case Study:

POWERFUL PORTAL

Web-based alerting and collaboration tool proves effective in presidential debate.

When President George W. Bush and Sen. John Kerry traveled to St. Louis to square off in the Oct. 8 presidential debate, scores of law enforcement organizations had to be coordinated behind the scenes.

These occasions traditionally spawn organized chaos as multiple agencies react to rapidly changing conditions using telephones and paper task orders. But this time, a collaboration portal deployed by the Missouri Office of Homeland Security strengthened and streamlined management of security for the high-profile event.

The Web-based collaboration tool, built with Microsoft SharePoint technology, coordinated activities of 25 state, local and federal agencies, including the U.S. Secret Service and the FBI. Commanders tracked the progress of events and the deployment of resources through the portal. XML forms were used to automate the paper-based process for assigning duties to 450 police officers deployed at the debate.

The event posed the first real-world test for the portal, which is designed to promote cooperation among the

diverse agencies that form Missouri's homeland security community.

The portal's initial performance earned sparkling reviews, said Tim Daniel, Missouri's homeland security director. "It was received extremely positively by the people in St. Louis," he said.

Solving Challenges

Building collaboration is a key challenge for Daniel, who became the country's first state-level homeland security director in 2001. His office coordinates activities of thousands of potential stakeholders to deter terrorism and respond to disasters.

Daniel needs to stitch together a remarkably diverse group of agencies and individuals — police, firefighters, doctors, emergency medical personnel and others. These stakeholders are scattered across the state, and they often have little in common, both culturally and technologically.

The portal responds to these requirements. Working with Convergence Communications, a Microsoft partner based in St. Louis, the Missouri Office of Homeland Security deployed advanced Web-based alerting and collaboration tools to flexibly meet the needs of this extensive audience.

"The central idea behind the portal is to attract people who have an interest in homeland security and enable them to act on that interest," said Daniel, a retired U.S. Army colonel. "I was looking for a vehicle that would let us communicate top-down and bottom-up at the same time."

Laying the Groundwork

Convergence Communications used Microsoft technology to create a portal capable of alerting as many as 10,000 participants within one hour through voice calling, text messaging, e-mail and paging. The portal also delivers collaboration functions such as e-mail, forums, calendars, shared documents, task lists and messaging that allow homeland security stakeholders to work together efficiently and effectively.

"When you look at all the people who could be involved in homeland security efforts, it's a huge audience. Getting all of them on the same page is a huge challenge," said Robert Wolf, president of Convergence. "The portal is the glue that will hold them together. It's the one system they all can have."

That was the case for the collection of state, local and federal agencies that provided security for the St. Louis presidential debate.

"All of the collaboration — as they worked with maps, documents, plans and even the discussions — took place in the portal," said Wolf. "Commanders could see what tasks are coming due, what had been accomplished and what was past due. This increased the situation awareness of the commanders and leaders."



Technology requirements are extremely minimal; users need only a browser and an Internet connection to access the portal. That's important because IT capabilities vary widely among stakeholder groups. An online registration process authenticates users and allows the portal to tailor information for users based on their roles and responsibilities.

The portal provides Web sites for individual agencies across Missouri's nine homeland security regions to promote internal collaboration. These agency-level sites are linked together to promote regional and inter-agency collaboration.

Demonstrating Effectiveness

The portal's success in the Oct. 8 debate sparked interest among other Missouri agencies, Daniel said. For instance, he expects the portal to support collaboration among 43 St. Louis-area hospitals that have partnered under a joint medical command.

"That group represents real progress," he said. "I'm looking forward to them using this tool to become even better in their communication and collaboration."

With basic communication and collaboration capabilities now deployed, Daniel expects users to mold the portal to fit their needs.

Fortunately the portal's SharePoint technology offers ample flexibility to meet evolving requirements. New applications can be built quickly, and deploying them is a drag-and-drop operation, according to Wolf. Furthermore, specialized Web sites can be created on the fly to manage events or support additional communities of interest.

Ultimately the portal's usefulness to homeland security stakeholders will determine its success.

"I can't just deem it to be successful. We're going to build it, and hope that users come," Daniel said. "Early indications are that portal use will grow rapidly. I'm seeking a network of networks, and I'm very hopeful this will find a life of its own."

Case Study:

ADVANCED PROTECTION

Michigan Health Alert Network enables rapid response to health threats.

Last March, a jetliner touched down at Detroit's Metropolitan Wayne County Airport carrying a passenger with a case of infectious measles. Everyone aboard the plane was exposed to the disease and needed an immunization within 48 hours to avoid a potential epidemic.

Working from his home computer on a Saturday night, the public information officer for the Michigan Department of Community Health immediately logged on to the state's Health Alert Network and notified local health departments statewide of the emergency. Within two hours, more than half of the local departments confirmed they had received the information. Within 24 hours, 98 percent of local officials had acknowledged the alert and were tracking down passengers for an inoculation.

"Those response rates with our local health departments are just outstanding," said Bill Colville, Health Alert Network coordinator for the Michigan Department of Community Health. "This network really brings together our public and private health-care communities in the state for emergency response."

Michigan completed the network in June 2003, working with Virtual Alert, a Sacramento, Calif.-based Microsoft partner that specializes in public health and safety solutions. Virtual Alert's Bioterrorism Readiness Suite (BTRS) is a Web-based Health Alert Network that was deployed in about four months and now connects more than 2,000 users at state and local health departments, private hospitals and Emergency Management.

Targeted Alerts

Using role-based directory technology, network users can send alerts to health-care officials throughout the state based on their position or geographic location. For example, an alert can target all epidemiologists in Michigan, or all health-care officials in a particular county.

The network uses multiple communication channels — e-mail, office phone, home phone, mobile phone or text message — to ensure alerts reach intended recipients. Users also may share and collaborate on documents such as emergency response plans through the system's document library.

"We didn't only build this network to meet immediate needs; we designed it to be a foundation for the future,"

said Virtual Alert's Dan Desmond. "This basically becomes the infrastructure for public health — for communication, collaboration and sharing of information."

The Michigan Health Alert Network — hosted at Virtual Alert's Sacramento facility, with a backup site in Austin, Texas — relies on Microsoft Active Directory for role-based access and messaging capabilities, and on Microsoft SharePoint Portal Server for Web-based communication and collaboration. "The combination of those technologies make this a very powerful tool and enables us to bring customers online quickly," said Desmond.

Local Support

The state manages the Michigan Health Alert Network, but it's also designed to support local public health departments. Local emergency preparedness coordinators have alerting rights similar to state agencies, and use the infrastructure to conduct their own operations.

"That creates a great sense of ownership in the system," Colville said. "It's viewed as much less of a 'state' system and more of a tool for the locals to use for their own notification needs."

Michigan simplified management of the network by making users responsible for updating their contact information. Every 30 days, the network automatically asks users for updated information when they log on to the system.

Users also specify which modes of communication to use for varying levels of alerts. Low-priority messages may be sent to work phones or e-mail addresses, while high-priority alerts could be sent to a pagers, mobile phones and home phones.

After each alert, the state Department of Community Health works with local Health Alert Network coordinators to weed out incorrect phone numbers or e-mail addresses. "We have a fairly elaborate quality control process," Colville said. "When we send out messages to 2,000 people, we get very little garbage back."

The network gives Michigan a powerful, flexible tool for protecting citizens from hazards ranging from infectious diseases to bioterrorism attacks. "This project has been quite successful," Colville said. "We're much better prepared to respond to public health threats."

Microsoft®

To learn how Microsoft solutions for government can help your organization, please visit us at www.microsoft.com/usa/government. Or call the Microsoft sales office at 800.426.9400.

This *Government Technology's Public CIO* Thought Leadership Profile was sponsored by Microsoft. Copyright © 2005 *Government Technology's Public CIO*. All rights reserved. Printed in USA.