



ADVERTISEMENT

On your mark, get set...

Agencies struggle to protect their data at all times

By Judi Hasson

Published on November 21, 2005

As the rain and the wind bore down on New Orleans, the Department of Veterans Affairs Medical Center tried to implement its disaster recovery plan before Hurricane Katrina hit town.

Officials attempted to download electronic medical records but were forced to copy them onto tape because the computer system had been knocked off-line. They rushed the tapes to Houston, where many hurricane victims relocated, but found that the tapes were not compatible with the systems there. So they had to scramble to reconfigure the computer systems to read the records.

Under federal law, every agency is supposed to have a contingency plan to protect their information technology systems. Whether it is a hurricane, earthquake, nuclear plant accident, terrorist attack or pandemic, agencies must be ready for any emergency.

Under the 2002 Federal Information Security Management Act (FISMA), agencies receive annual reviews on the status of their plan and whether they have tested it. They are also subject to continuity of operations planning directives developed by the National Institute of Standards and Technology, which require agencies to activate a recovery plan within 12 hours after a disaster.

Many praised VA officials for their evacuation efforts after the storm. But at a congressional hearing in September, VA officials said they fell behind in dealing with electronic records.

"We had to take the tape to Houston, install it, configure it in Houston and bring it up," said Robert McFarland, the VA's chief information officer, while testifying before the House Veterans' Affairs Committee Sept. 14. He said a regional data-processing system would have eliminated that obstacle.

Rep. Michael Bilirakis (R-Fla.) found the problem outrageous. "You had to reconfigure the Houston computers? You had to reconfigure it at that point in time?" Bilirakis asked McFarland.

Many government disaster recovery plans are only half done or completely unacceptable. In February, Rep. Tom Davis (R-Va.), chairman of the House Government Reform Committee, gave the federal government poor grades on securing electronic information systems.

But the Katrina catastrophe, followed by Hurricane Rita, gave the federal government a wake-up call about the importance of securing information and making sure agencies are ready to resume operations immediately after a disaster.

Karen Evans, administrator of e-government and IT at the Office of Management and Budget, said federal agencies have not consistently met their obligations to protect their records. But they are improving.

Agencies recently submitted their 2005 reporting requirements to OMB, which oversees contingency planning for federal IT systems and uses the FISMA reporting process and the President's Management Agenda score card to monitor agency efforts. The FISMA report will be available in March 2006.

In "the past several years, agency performance has been mixed but continues to improve," Evans wrote in an e-mail.

In June OMB issued an order requiring agencies to make sure they could maintain telecommunications services during a crisis or emergency. At the same time, Evans added in her e-mail message that only slightly more than half of the agencies reporting in 2004 had tested their contingency plans. OMB continues to monitor their progress, she said.

"OMB has responsibility for overseeing contingency planning for federal IT systems and uses the FISMA reporting process as well as the President's Management Agenda score card to monitor agency efforts," she said in her e-mail.

In some cases, agency performance has been spectacular. While the VA was having trouble with its records, the National Finance Center, which pays 565,000 federal workers from more than 130 agencies every two weeks, activated its disaster plan and moved its operations from New Orleans to Philadelphia before Katrina hit. The delivery of paychecks never stopped despite the chaos, said Jerry Lohfink, the center's director.

Lohfink said the center has an operational disaster recovery plan and practices it many times during the year, regularly as a computer-based exercise and twice a year as a full-fledged drill. As part of the procedure, the center has established checkpoints where employees can get updates during a disaster and has mandated that employees regularly call to report their locations.

"You knew you had this responsibility," he said. "It avoided the mayhem. It allowed us to overcome infrastructure issues like the lack of landlines. People knew what the plans were, and it allowed an orderly conduct of business in the midst of the disarray of the storm."

Marianne Swanson, NIST's senior adviser for IT security management, said agencies are supposed to have an IT contingency plan for each computer system, but "the depth of the contingency plan depends on the system."

"If it's for an earthquake or blackout, you can do tabletop exercises, go through scenarios and have supplies," said Swanson, co-author of NIST's "Contingency Planning Guide for Information Technology Systems."

"You can shake out a lot by doing a tabletop exercise," she said.

The Department of Housing and Urban Development didn't waste any time when the weather reports predicted a nearly direct hit for New Orleans, HUD CIO Lisa Schlosser said.

"We have taken a 'prevent and recovery approach,'" said Schlosser, whose agency is now responsible for providing housing for 400,000 dislocated families. "We had a standard 'go' kit with a [Research in Motion] BlackBerry and a laptop with a wireless connection. We've been sending out 30 business folks to assess damage."

Meanwhile, the Navy's Systems Center in New Orleans, operated by the Space and Naval Warfare Systems Command, had been watching Katrina's path. It began transferring payroll information, personnel data and the system that records personnel orders to Fort Worth, Texas, two days before Katrina hit, said Capt. Fred Mingo, who is in charge of the New Orleans center.

The center conducts annual drills on how to transfer all data to another site, he said. Each exercise identifies problems.

In the real-life situation, Mingo said, no one could reach him on his cell phone, which has a New Orleans area code, because Katrina knocked out

most cellular towers.

It was an important lesson learned, he said, and next time, "a couple of things will be different. There will be much more phone capability, and cell phones will be issued with different area codes."

Nevertheless, agencies vary in compliance with disaster recovery requirements. The U.S. Patent and Trademark Office is one agency that is running behind in developing an IT contingency plan. In the next year, the agency intends to set up "multiple, geographically dispersed data centers that would allow for operations to be switched to an alternate site in the event of a catastrophic failure of the primary data center," said spokeswoman Bridget Quinn.

She said USPTO cannot get its primary computer and network systems back in operation within 12 hours as required but could operate using paper files if it had to.

Lynn McNulty, director of government affairs at the International Information Systems Security Certification Consortium and a former NIST manager, said the problems that the federal government is experiencing have happened because it did not take risk management seriously.

"Contingency planning and continuity of operations has been one of the least paid attention to of the whole comprehensive security problem out there," McNulty said. "I've seen a lot of people go through the motions of writing contingency plans. Then they sit on the shelf, never get tested. As a result, when the emergency [comes], their continuity plan is not up to speed, their staff hasn't been trained, and they are not ready."

Evans said the federal government is working hard to fill in the gaps. "The hurricanes certainly reinforced the need for viable continuity of operations plans. OMB, in conjunction with the Department of Homeland Security, continues to review agency plans to protect their critical cyber infrastructures," Evans wrote in an e-mail.