



Virtual IT, Inc.

Case Study – City of Lynchburg, Disaster Recovery

Overview:

“The disaster recovery plan we had wasn’t workable,” says Mike Goetz, looking back at his department at the beginning of 2005. Goetz is Director of Information Technology for the City of Lynchburg, in central Virginia. “It was several years old, had not been maintained, and our environment had changed – with new computers, new systems, and the addition of new hardware and software.”

Adding to the situation, he says, was the fact that a recent external audit noted that “the plan we had didn’t describe reality.” As a result of the audit, a commitment was made: develop a credible plan by the end of the fiscal year.

Challenges:

One of the IT department’s biggest challenges was sheer growth. People and organizations are taking more and more advantage of IT, says Goetz. “It’s the way of the world.”

The growing complexity of the department quickly rendered the current disaster recovery plan inadequate. He gives several recent examples of this growth, including: a new system to assist building inspectors and community planning, additional tools to block spam and prevent viruses, and a new system for city real estate appraisers. “All of this is located in our data center,” he says. The scope of the plan was becoming enormous; concern was growing about what to do if the data center was destroyed.

Solution:

“Virtual IT led the development of our plan,” says Goetz. “They gathered data, analyzed it, created the plan and validated it.”

“They held a series of interviews and working sessions with small groups, focusing on systems and devices, in order to build an inventory and determine how these systems are inter-related. “In order to recover them, you have to understand them,” he says. “Part of the conversation also included risk assessment and prioritization.” Approximately twenty City staffers participated in the process.

As a result, a five-tier framework was established. Tiers One and Two identified those critical systems which needed to be recovered within 72 hours. “That drives us to identify where to physically locate hardware,” says Goetz. “We identified a second site, along with 15 hardware devices that needed to be replicated in that site to meet the required recovery time frame.”

Tiers Three, Four, and Five identified systems which required recovery ranging from within one week to one month. “These called for a different strategy,” he says.

Results:

“Virtual IT met our requirements – a structured plan for recovering applications and systems, by the end of our fiscal year,” says Goetz. “They hit the mark – on time – and they did it well.”