

Ways to Win

Government IT faces new challenges with the rapidly expanding mobile work force.





Mobility and More

A tech-savvy county sees challenges — and solutions — brought on by an ever-expanding mobile work force.

Harris County, Texas, is one of the most populous counties in the United States. From its seat in Houston, the county government serves nearly 4 million residents. The county's IT staff supports more than 16,000 employees in 278 locations.

That's a big job in itself, and it's growing more challenging every day with the rise in the number of mobile workers. With today's network boundaries often extending well beyond traditional perimeters, IT departments deliver information and applications further out than ever before. They also must protect data and computing assets wherever they are.

So how do you do it? Steve Jennings, CIO of Harris County, said the Harris County Information Technology Center (ITC) focuses on four key points: creating a robust and secure infrastructure to ensure bandwidth availability; modernizing application delivery; thinking harder about the data itself, including where it comes from, where it needs to go, and how to secure it; and re-orienting the organizational culture to adapt to the realities of increased mobility and a new generation of workers joining the public sector.

Flexible Infrastructure

Harris County's network is a Converged Information Utility (CIU) with high-speed switching, large bandwidth and centralized management. Many of its services and applications are enabled or enhanced by Alcatel-Lucent technology. It's a robust network that allows for converging data, video and voice for maximum efficiency.

"We believe we should have a flexible, fluid network to fit the needs of our customers," said Jennings. "And each customer is different."

Bandwidth traditionally has served brick-and-mortar facilities, Jennings noted. Now what's needed is greater flexibility. The CIU delivers those capabilities, enabling communications convergence and providing opportunities for virtualization of computers, servers and databases.

Now it's easier for Jennings to give the county's mobile workers access to the data they need in order to be productive. But access must be balanced with security. And security issues grow more complex as more mobile devices are used and the need for protection expands to potentially thousands of remote endpoints.

Ways to Win

The new mobile work force presents opportunities never seen before. Technology now enables workers to be immersed in productive business while not at the office. Employees can take computers, applications and mountains of data with them — and be productive from almost anywhere.

However, expanding the endpoints of an IT network far beyond traditional perimeters brings new risks and issues. How do you provide greater access to data and still keep that data secure? How do you protect against lost or stolen laptops? How do you embrace the Millennials in your work force — a technology-savvy generation that's grown up with computers, but not with the structured methods leveraged by government?

Governments face numerous other challenges too, including loss of property tax revenue due to the mortgage market, loss of tax revenue thanks to layoffs, and higher fuel costs. Budget constraints make it harder to expand services.

Fortunately IT staffs are coming up with creative solutions. They're leveraging technology in new ways, and extending their network reach further than ever before. Many are looking at new service delivery models to support ever-increasing "always on" communications.

Growing numbers of mobile employees want the same capabilities they have in the office. There are many productivity, cost and environmental benefits to giving them these resources. But shrinking budgets, regulatory requirements, security issues and other challenges must be dealt with.

Government *can* win. The following case study dives deeper into these issues, and shows how one county is managing the challenges brought about by today's — and tomorrow's — new mobile work force.

Jennings sees a need to rethink security, since traditional efforts have been geared to permanent physical locations and hardwire connectivity. The data is critical. You need to know where all your data is, and you need to manage it well. “Really, your key asset is your information,” Jennings said.

It’s important to understand who needs the data, where it’s supposed to go, and how it’s utilized. Extra care must be taken with sensitive data like justice, financial or health records. Regulatory requirements including HIPAA (Health Insurance Portability and Accountability Act) must be observed. It all requires diligent management of the information.

To protect data on lost or stolen laptops, Harris County’s ITC is testing Alcatel-Lucent’s OmniAccess 3500 Nonstop Laptop Guardian developed by Bell Labs, and Jennings likes what he sees. The security solution allows centralized management of remote laptops by communicating with a self-powered wireless PC Card plugged into each laptop. Now IT staff can safeguard the sensitive data on employees’ laptops anytime, anywhere, even when the laptop is powered off. From off-hour downloads of patches and updates, to backups and proactive, real-time response to security loopholes arising through public Internet access, the Nonstop Laptop Guardian increases productivity, helps enforce

“The biggest thing is understanding the Millennial culture. And it’s going to be a balancing act.”

Steve Jennings, CIO, Harris County, Texas



100 percent IT policy compliance and improves business continuity. With third-party integration, Harris County intends to use the system to recognize when the laptop has gone outside its “geographic fence,” allowing IT staff to lock down the machine and remove access to encrypted content — whether the machine is turned on or off. The Nonstop Laptop Guardian is just one example of a new technology that can help government stay on top of the issues that come with increased mobility.

New Delivery Methods

The county also is redeveloping its application delivery. It’s looking closely at the requirements of mobile workers. Information must be streamed out to increasingly smaller devices in a powerful way. One solution for Harris County is to do more with video. That allows a building inspector, for example, to give a more comprehensive report from the field.

The new emphasis on mobility also impacts recruiting — and will for years to come — as a new generation of young employees joins the work force. Known as Millennials, these workers — who are ages 15-25 now — will want to work for government if innovation is embraced and the environment is not too limiting or regimented. And they like to be mobile.

“I call them the Triple-A’s,” Jennings said. “They’re the Anytime, Anywhere, Anyhow work force. That’s literally what your future work force is going to be.” Millennials are used to being online and getting things done from all kinds of locations, on all kinds of devices.



Jennings acknowledged that some Millennials are known for being undisciplined, or not following standard processes. But the group is also known for being collaborative, and Jennings sees a lot of potential there. "As long as you can make them part of the solution, instead of dictating to them what the solution is, the reality is they're going to be a lot more adaptive," he said.

Millennials are into texting, YouTube, wikis and other new ways to communicate. "We're going to also have to adapt, and utilize these tools, and be flexible in how we bring them into our solution set," said Jennings. "The biggest thing is understanding the Millennial culture. And it's going to be a balancing act."

Of course, balancing anything is easier with more funds. But that's not the reality in today's economy. Jennings said

tough times can lead to more efficient, enterprise approaches instead of departmental ones. Government agencies need to work smarter, more efficiently and be cost-effective.

"You have to get more creative," Jennings said. "But it's also a good time for technology because a lot of times, it's technology that is the glue that brings various solution sets together."

Changing Attitudes

As for the change of organizational culture, understanding the new mobile worker is vital, Jennings said. Retraining and re-evaluation of existing staff will be needed. Mobile workers are managed less and are more on their own in the field. That may require a new structure of management metrics in some cases.

Understanding security concerns and processes can be a nuisance for end-users. A system that can automatically connect a VPN session, deliver patches, updates and commands and be remotely managed by IT even during off-hours is ideal for mobile workers. Solutions such as Alcatel-Lucent's OmniAccess 3500 Nonstop Laptop Guardian can provide the 24/7 monitoring, visibility and control — leaving employees responsible only for reporting laptops if lost or stolen.

It's now more critical than ever before to find the right blend of data accessibility, dynamic technology and strong security to optimize your operation. Jennings pointed out that you can't focus too much on one area, because that could leave a huge gap somewhere else. "The reality is, you can't just do one function by itself," he said.

As Harris County moves into the future, mobility will continue to contribute to productivity. Coping with growing mobility requires creative solutions, but the fundamentals remain extremely important. "We're really getting down to the three basic cornerstones: people, process and technology," said Jennings. "People and process are going to be absolutely critical in the new mobile work force."



Alcatel-Lucent delivers complete, best-in-class communications solutions aligned with the most challenging mission imperatives of government, and tailored to business needs. Alcatel-Lucent: serving those who serve the public in an always-on world.

For more information
visit <http://www1.alcatel-lucent.com/us/slg/>
or call 1-800-252-2835



Advances in Laptop Security Allow IT Management to:

- **Secure laptop data**, access and management through always-on 3G communications
- **Gain 24/7 visibility and control** through an independent, trusted and verifiable platform
- **Reduce liability** of lost or stolen laptops with remote backup, wipe and kill capabilities
- **Improve business continuity** with real-time responses to virus and worm threats
- **Increase productivity and compliance** through off-hours patch downloads and backups