BANK SYSTEMS & TECHNOLOGY

October 1, 2005

Work Without Wires -- Most companies are content with a couple of Wi-Fi conference rooms, but Capital One thinks a wireless campus will spur game-changing brainstorms. Is it time to reconsider the potential of wireless?

BYLINE: Elena Malykhina

For some 1,500 employees and contractors working for McLean, Va.-based Capital One Financial Corp., the desk has gone the way of other office dinosaurs, like the typewriter. The first wave of the company's knowledge workers to be outfitted with Wi-Fi enabled laptops, Voice over IP software phones and portable printers now can do business from anywhere within Capital One's 24 buildings in the United States and the United Kingdom.

These employees are the first in a program Capital One calls "Future of Work," which CIO **Gregor Bailar** defines as a necessary step in keeping the $1.5 billion-a-year bank and credit card company competitive. "The Capital One story has always been to look for the game-changing opportunities," Bailar says. Capital One's staff at large uses a Web portal that routes work processes to employees automatically, making it easy for mobile professionals to do their jobs from any location.

The people, who Capital One selected from its 15,000 employees to participate in the program, which launched last fall, work in information-intensive areas such as finance, human resources and IT. Bailar expects 1,000 more employees to become mobile users by the end of next year. Already, the company reports that the program is helping achieve the three critical goals for which it was designed: keeping employees satisfied with their jobs, improving productivity and reducing costs related to real estate.

Capital One's Future of Work program is ambitious. It extends from stand-alone buildings to a 360-acre, eight-building campus with wireless access points covering coffee rooms, cafeterias, and more-traditional work spaces such as offices and conference rooms.

While Forrester Research (Cambridge, Mass.) predicts that 64 percent of U.S. companies are upgrading or deploying wireless LANs in 2005, just a small percentage of those are multi-campus deployments that provide wireless access to large portions of a company's workforce. Most IT execs still don't buy the argument that large wireless network deployments can provide a productivity boost that justifies the security and management headaches and extra expense.

Because of the increasing number of public Wi-Fi hot spots, however, people are growing more accustomed to the convenience of connecting wirelessly. The number of publicly available hot spots in North America will reach 20,400 this year, according to research firm Gartner (Stamford, Conn.); the Yankee Group (Boston) predicts that 1.5 million people will pay to use commercial Wi-Fi hot spots by the end of this year; and components of wireless infrastructures are creeping into the workplace as more businesses choose wireless-ready laptops and PDAs when making upgrades.

Factors Keeping Wireless Grounded

But there are challenges to unplugging a company's workforce. Though equipment prices are declining, many companies still find it difficult to justify the cost of a full-blown wireless infrastructure when the wires in place work just fine.

Capital One declines to put a price tag on its initiative, but the cost of access-point hardware to support 12 users is about $800. Forrester says companies can expect to spend $3,000 per switch, $9,000 for a management tool and $8,000 for intrusion-prevention software to secure wireless networks, which inherently are easier to piggyback on or crack into than are wired LANs - threats include employees installing unsecured access points without the IT department's knowledge and competitors scanning buildings from parked cars.

The fact that most vendors haven't consolidated wired and wireless network management tools also inhibits large-scale wireless implementations, forcing companies to deploy different systems to monitor wireless LANs. Generally, they also have to manage each campus wireless LAN separately, although that's changing with the increasing availability of wireless LANs that can be managed centrally.

Further, to realize productivity gains, a company must establish processes to support working online. Capital One established a Web portal through which employees access the company's PeopleSoft (Redwood Shores, Calif.) and other workflow applications. "People expect things to happen fast, to be efficient, to be working toward workflows instead of moving paper around," Bailar says.

Microsoft Provides an Example

Among the leaders in deploying wireless LANs, Microsoft (Redmond, Wash.) offers an example for financial services firms considering establishing a wireless workplace. The company is replacing a global wireless LAN infrastructure with an even larger one that will encompass 277 buildings worldwide and cover more than 17 million square feet, a project expected to take up to two years to complete. Microsoft is deploying 5,000 "thin" wireless access points from Aruba Wireless Networks (Sunnyvale, Calif.) that can be managed centrally and will provide connectivity to an estimated 100,000 computing devices. It's one of the largest, if not the largest, wireless LAN deployments in the world, according to Craig Mathias, an analyst with wireless consulting firm Farpoint Group (Ashland, Mass.).

Microsoft has been using Cisco Systems (San Jose, Calif.) equipment, which requires device management at each access point. Growing demand for centralized tools to manage wireless LANs prompted Cisco to offer a thin-access-point setup through its recent acquisition of Airespace (San Jose, Calif.). Other wireless LAN vendors, including Extreme Networks (Santa Clara, Calif.) and Trapeze Networks (Pleasanton, Calif.), offer their own approaches to central management, which makes it easier to expand networks and can reduce costs because less equipment is needed, Mathias says.

Though Capital One, citing security concerns, won't discuss its network-management approach or reveal its wireless vendors, Future of Work already is providing benefits. Since the deployment, Capital One's buildings accommodate more people. For example, its West Creek campus near Richmond, Va., used to house 650 employees. With Future of Work, the number of people working there jumped to 1,100, simply by reconfiguring the office space.

Security Concerns

But such large-scale wireless deployments raise security concerns, and with good reason - the Wired Equivalent Privacy protocol, predecessor to the 802.11i standard ratified last year, has been shown to have serious flaws that can be exploited, and its weak authentication methods have made wireless networks vulnerable to attacks. Capital One and Microsoft hope to avoid these problems by using 802.11i-compliant equipment. The standard defines a

method, called Wi-Fi Protected Access 2, or WPA2, for authenticating and encrypting wireless LANs.

At the heart of Microsoft's wireless LAN deployment is Aruba's switching system, which centralizes 802.11i security functions, including wireless encryption, authentication and user-access controls. This means Microsoft will be able to control and encrypt all its wireless devices centrally. Aruba CEO Don LeBeau believes a combination of centralized control and tight security is what many businesses will require in wireless LANs.

Revenue for the worldwide, wireless LAN security market is expected to reach $279 million by 2009, compared with $41 million in 2002, according to a new report from research firm Research and Markets (Dublin, Ireland). Capital One has built a "rigorous security infrastructure" that includes an enterprise wide intrusion-detection system, Capital One's Bailar notes. In addition to encrypting communications between the wireless network and mobile devices, Capital One enforces security policies, such as minimum password length and limits on the number of unsuccessful log-ins from centralized servers.

LAN Management

Security challenges aside, wireless LAN management remain an issue. "The whole network-management space still needs a lot of work," Farpoint's Mathias says.

Insufficiently managed networks can result in increased security risks, higher operational costs and dissatisfied users. Computer Associates (Islandia, N.Y.), Hewlett-Packard (Palo Alto, Calif.) and IBM (Armonk, N.Y.) all promise network-management tools that can be used on wired and wireless networks, which should make it easier to manage both, according to Forrester analyst Ellen Daley.

For the IT help desk, wireless networks can be difficult to troubleshoot. If users have a problem connecting, they'll often move to another area covered by a different access point, impeding the help desk's ability to determine the problem, Capital One's Bailar says. And there are inexplicable occurrences with wireless networks - in one instance, the Capital One help desk discovered interference with one of its access points but couldn't determine from where it was coming. It was learned later that a user had introduced a device into the wireless LAN environment that wasn't owned or approved for use by Capital One, and the device was utilizing the same spectrum as the network.

Despite these challenges, the momentum for wireless is continuing to gain speed. Wireless LANs will evolve to support more emerging applications, such as Voice over Wi-Fi, which Capital One envisions giving its mobile workers even more flexibility down the road.

Ultimately, employees will demand a wireless workplace. New hires are coming from college campuses with Wi-Fi everywhere. Everyone already can get Internet access on planes and have wireless access served up with mocha lattes at Starbucks. Fewer businesses will be able to offer wireless access only to employees away from the office, and many more will have to provide it to employees on home turf, too.

Copyright (c) 2005 CMP Media LLC. All rights reserved.