BUFFALO
BUSINESS FIRST
WESTERN NEW YORK'S BUSINESS NEWSPAPER

Friday, March 3, 2006

Let's get unwired

Ever-expanding wireless communities bring new opportunities and expectations

Business First of Buffalo - by Tracey Drury Business First

Everywhere we look, people are taking advantage of wireless technology to communicate, stay in touch and keep up with business affairs.

Besides the almost universal presence of cell phones wielded by people of all ages, laptop computers, Blackberry devices and other personal digital assistants are being used nearly everywhere. That includes outdoor parks, hospitals and jury rooms.

Professionals say the increased use of wireless devices has given rise to new issues in the areas of both security and privacy, issues that aren't as readily obvious to the everyday person.

"We have become used to being part of a wireless community," said Michael Connally, vice president of sales at **IPLogic**, who was among a group of technology professionals who participated in a recent roundtable discussion at Business First.

Over the past year, as wireless networks expand in both public and private domains, people have come to expect a certain level of service or at least accessibility. Danny O'Dea, major account manager at **PremCom Corp.**, said it's to the point where he expects a seamless transition for communication.

"When I want to walk outside the building, when I want to take my PDA or my phone, I want the seamless phone scenario," he said. "It's really changed and morphed in the last year, what the concept of wireless is."

Joining in

What's happening in many cases is wireless communities are starting as the creation of a specific community for a common purpose, whether that's commercial, educational or otherwise. Others come in looking to become a part of that community, Connally said.

"You start to look for other, larger communities and that's where the security part comes in," he said. "In my workplace I have it, but when I'm in someone else's workplace or sitting here in this conference room, I'll see if there's another wireless community someone else has built for me, whether I'm invited or not."

Tony Klejna, director of educational technology at **Daemen College**, said the big issue he's had to deal with is how much access to provide to students, while keeping the campus systems

safe. With more than 50 wireless access points around campus, students and staff have the ability sit out under a tree for class or study on their own in the library.

"It's not always secured so that's a big question for everyone, especially when you have a public network," he said. "How much do you let in? How much are you going to firewall? We don't do a lot of that. One of the goals we have is to be able to take your tablet or PDA and wander around campus and not have to authenticate 10 times. We're making slow, but sure, progress."

The University at Buffalo is dealing with similar issues, but with 350 access points the issue is magnified, said Frederick Wood, UB associate director for communication services.

"Every time you move, you need to authenticate," he said. "We've been trying to enhance that at the university."

The organization is left to struggle with the issue of whether to let others use the network, and if so, how to do it without jeopardizing sensitive internal data on the network.

"It's another set of struggles. As these communities are getting larger and larger, and of course, municipalities are looking to create these communities that invite people to do business in their community," Connally said.

The numbers of people signing up to use these municipal and other community networks illustrates just how popular they are becoming, said Les Hoffman, director of information and support services with the Erie County Industrial Development Agency.

Hoffman has worked with InfoTech Niagara, municipalities and tech providers to set up the Buffalo-Niagara Wi-Fi initiative, which offers free wireless access for computer users in over a dozen places throughout the region.

"Everyone wants to be part of a wireless community," he said. "Our vision is that you can go anywhere in Buffalo Niagara. We're also trying to at least raise consciousness about the issue."

Hoffman said the collaborative has not seen any issues arise concerning liability since the Internet connection is muzzled somewhat by restricting downloads and pornography using filters. The project is also set up in such a way that it does not compete with Internet providers in the region.

"That keeps us in good stead with the ISP providers so they become our sponsors rather than viewing us as competitors," Hoffman said. "We're providing an amenity and putting the Internet out there. If you really want to use the Internet, you're going to want to have your own service."

Those areas that are still without wireless access hold out hope that Verizon will expand its broadband wireless service to communities such as East Aurora, said Jeff McCaskey, president of **Aurora Consulting Group Inc.** Although his company has its own wireless network, as do many other area businesses, it's still not available to the public.

"There's no access there for people who want that sort of thing," he said.

Keeping systems safe

The next step for providers and communities will be how to protect their internal networks from too much traffic slowing things down, as well as viruses and individuals trying to sneak a peek at internal documents.

Connally of IPLogic, said there's a fine balance to enabling access and keeping the system efficient.

"How are you protecting that information and how to protect that user without making it arduous?" he said.

Some users fail to realize that when they are connected through a wireless network, they are just as exposed as everyone else out there, and may not worry about protecting their own information.

The same is true in instances where someone installs a rogue access point for their own private use, but which then exposes the company's entire network.

"It's not just the host or the person who's providing the wireless access, but it's also the individual who says 'I can't wait to have access while I'm sitting at my doctor's office'," Connally said. "The security issues are abundant on both sides of the equation. People fail to realize that."