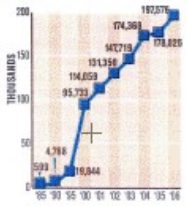
In Depth:
WIRELESS TECHNOLOGY

Charting it out

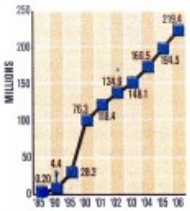
CTIA-The Wireless Association, an organization representing all sectors of wireless communications, conducts a semi-annual industry survey. Below are the results from June 2006.

Cell sites



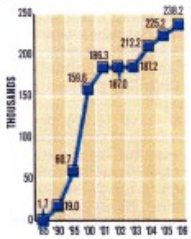
The cell site survey reflects domestic, commercially-operational cellular, ESMR and PCS providers.

Wireless subscribers



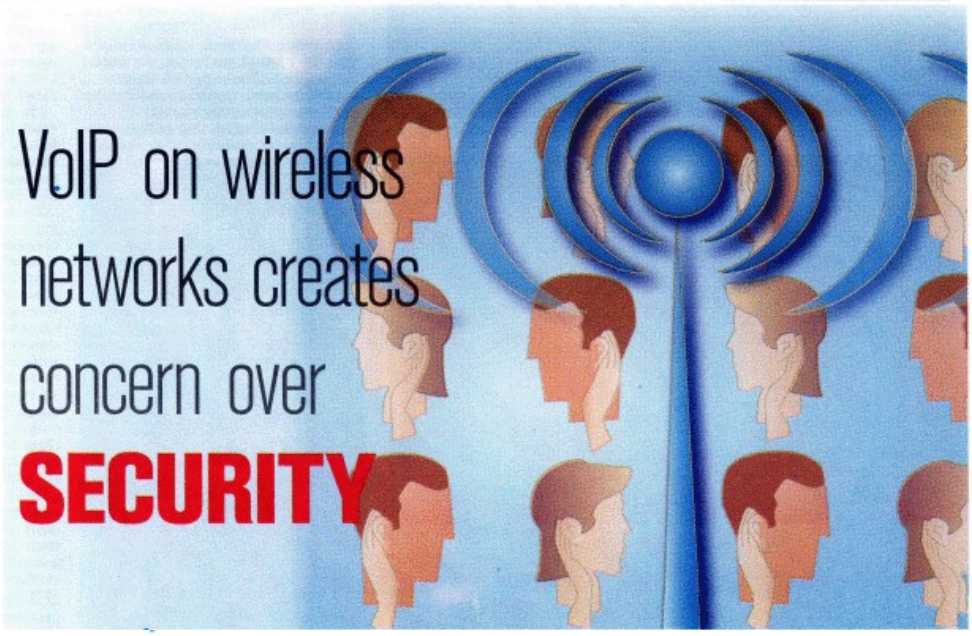
Subscribers are measured by the number of wireless accounts, or subscriptions.

Wireless employment



Direct wireless carrier employment grew 6 percent from June 2005 to June 2006.

SOURCE: CTIA – THE WIRELESS ASSOCIATION



Voice and data come together, but open door to snooping

TIMOTHY ROBERTS
troberts@bizjournals.com

Wireless networks aren't just for data anymore, and that fact has security experts worried.

An increasing number of companies are adding voice over Internet Protocol (VoIP) to their wireless networks, and the convergence of voice and data on these systems has created a bigger security problem. The biggest threat is that more people will make greater use of the network from more places — and some of the connections they use probably will turn out to be questionable.

The size of the market underscores the urgency for confronting the potential trouble. Infonetics estimates the market for wireless voice will grow from about $100 million now to about $1.9 billion by 2009.

Security concerns are heightened by recent corporate regulations.

"All the regulations like Sarbanes-Oxley apply to voice also," Chia-Chee Kuan, chief technology officer of AirMagnet Inc., told a panel Feb. 7 at the RSA Security conference in San Francisco.

Sarbanes-Oxley requires a CEO to sign off on company reports promising that they are accurate. That means the data in those reports can't be compromised by hackers.

And the stakes are getting higher. The FBI reports that the cost of data breaches in 2006 came to $62.7 billion. According to a report issued by Santa Clara-based computer security company McAfee Inc. at the RSA conference, the cost to Wells Fargo of notifying 33 million customers recently that their personal data may had been exposed was $19 million.

Wells Fargo was required to contact customers by a California law championed by State Sen. Joe Simitian, D-Palo Alto, who was awarded the RSA Conference Public Policy Award this year.

U.S. Sen. Dianne Feinstein of California has just introduced similar legislation in the Senate.

In an address at RSA, FTC Chairman Deborah Platt Majoras warned businesses that they must have "reasonable and appropriate measures in place" to protect any personal data they have collected on their customers. Although she didn't directly speak to the voice-over-wireless threat, she promised action by the FTC that will require businesses to be aware of threats to their security systems.

Phone handsets present a special challenge. Laptops using wireless networks can have sophisticated encryption, but telephone handsets generally don't have that kind of technology. What's worse is that only about 40 percent of wireless networks have any kind of security, says Gurminder Singh, the CTO of Shimon Systems Inc., a wireless security company in San Jose.

Shimon's answer to the security problem is a biometric system that uses a fingerprint reader attached to or built into a computer to identify the user. CEO Baldev Krishan predicts that biometric sensors like the one his company makes will soon be on a third of laptops and will begin appearing on cell phones too. They already have begun to appear on Japanese cell phones.

The voice-data convergence on wireless is helping to push the security focus away from the traditional perimeter defense to the end point like the laptop or WiFi phone.

Because of wireless networks, says Vimal Solanki, senior director of marketing at McAfee Inc., "We are working without borders. The network is wherever we are."

Every company with wireless should develop a way to enforce basic policies for employees out on the road, says Sri Sundaralingam, director of product management and technical marketing for AirTight Networks Inc. in Mountain View. These policies should include what networks employees should connect to.

Windows XP-based computers will connect automatically to whatever network has a good signal, Sundaralingam says, even if that network is a rogue set up to mine data. The Apple Inc. OSX operating system tells users if none of their trusted networks are available.

Of particular concern are the growing number of municipal networks, many of which are quite open and insecure. A VoIP call using one of these networks could be "sniffed" by someone hunting for information.

"The scariest thing is that with analog phone calls, you would have to tap into the telco system," Sundaralingam says. "With VoIP, you can be anywhere in the world."

TIMOTHY ROBERTS covers public policy, corporate governance and Internet security for the Business Journal. Reach him at (408) 299-1821.