

Mobile users share tips for best wireless security

By: Jim Duffy

Network World (07 Jul 2006)

Network professionals at last month's Globalcomm 2006 conference said they are exploiting the latest wireless and mobile technologies to get employees closer to customers and increase productivity, but are constantly facing new security challenges in doing so.

"You can connect more, but guess what? More direct attacks," said Andy Farkas, assistant vice-president of emerging technologies at Capmark Financial Group, a mortgage servicing company in Horsham, Pa. "More malware, more software patching [which] costs more money. So the more we give our employees to connect, the more vulnerabilities we're going to have to face."

Farkas delivered a keynote address at Globalcomm, a big new telecom industry show that grew out of the defunct Supercomm event. In addition to highlighting the latest mobile computing trends, the show featured announcements and demos from telecom service and equipment providers such as AT&T, which outlined plans to upgrade its MPLS backbone to 40Gbps speeds this summer.

In his address, Farkas described his company's extensive use of wireless. Capmark has 3,000 employees in 100 offices in nine countries. The company has a campus Wi-Fi--mesh network for data and voice, wireless video surveillance, point-to-point wireless between buildings for disaster recovery, and a mix of cellular technologies for WAN applications.

Employees use BlackBerry, Palm, Audiovox and Imate handheld devices to enter and retrieve loan information in back-office systems in Horsham through a Web-based portal written in Microsoft's .Net language. Implementing and supporting a mix of devices makes the IT department's job harder, but Farkas said that needs to be balanced with letting other employees do their jobs more effectively. "I just can't give one device and say, 'Everybody use the same thing,' because they have different levels of responsibility," he said.

Farkas said Microsoft's security features pack and Research In Motion's BlackBerry-Enterprise Server let devices be managed by policy, locked down, password-protected and cleared of sensitive data if they are lost. "We can remotely wipe them if somebody calls up and says, 'I left my phone in the cab,'" he said.

The increasingly mobile network has led to more attacks, though damage has been kept to a minimum through proactive measures, Farkas said. "We've employed things where if people are coming into our networks that we're checking anti-virus levels and firewalls and patching levels," he said. "We're making sure those things are turned on so we can protect our networks."

Protection was one reason Whirlpool, of Benton Harbor, Mich., decided to standardize on RIM's BlackBerry as its handheld mobile platform. Fewer than 25 per cent of Whirlpool's worldwide workforce of 88,000 is mobile, but that will increase dramatically over the next 24 to 30 months, said Rick Perrotta, director of global network engineering and services.

"The speeds-and-feeds part was fairly one-dimensional, but when you talk about the policy and application layer it's much more complex. It can really force some critical thinking around what the right corporate policies are and then how to enable them from an application standpoint," he said. A uniform platform makes it easier to define and employ security policies, Perrotta said.

Whirlpool is trying out AT&T's new managed RFID service to tag and track mobile users. "We're in the midst of really doing some good work around security strategy and methodology and capabilities that will bring us a significant level of control on what devices come and go from the network, and are they clean [or] not clean," Perrotta said. "[But] we view it as equal proactivity among all devices regardless of whether they are fixed or mobile."

Heightened mobility also has meant heightened awareness for Skywest Airlines of St. George, Utah. The company shares communications rooms with other airlines, and it continually has to monitor for rogue access points, said Kevin Simmons, director of system support. The company also requires its users go through layers of security clearances — authentication through a VPN client, RADIUS server and digital certificates — and has set up a separate Ethernet segment on its access point so crew members can use their own laptops.

In addition to the cyberthreats are physical ones. Sharing facilities with other airlines has resulted in some sabotage to Skywest access point equipment, Simmons said.