



# FINANCIAL IT SECURITY

March 2006

//networked//

## Policing WiFi Access

Detecting rogue access points is now mandatory, even in institutions that long-ago instituted "no wireless" policies. BY REBECCA SAUSNER

If you're still confident that your institution's long-held "no wireless" policy is protecting your corporate network from the real and perceived security risks of wireless LANs, it's probably time for a closer look. Chances are there are a dozen or more wireless access points inside your network, depending on the size of your facility, that promise drive-by access to any black hat with a laptop parked out front.

Richard Rushing, CSO of wireless security vendor AirDefense, loves to illustrate the point by conducting "war drives" through New York's financial district, picking out one insecure network after another. "People don't grasp how much you rely on physical security to protect your network," Rushing says, noting that the proliferation of easy-to-install wireless access points, not to mention access points built into new printers, projectors and other devices, means walls and firewalls are easily scaled.

"The idea that you could shove a \$79 access point onto a corporate network and use the PDA you got for your birthday to connect is very tempting," says Nick Selby, enterprise security analyst with The 451 Group. "Companies in financial services really need to know this is happening. Even if you haven't deployed Wi-Fi, it's becoming necessary to have some kind of Wi-Fi detection and prevention capability."

Though there are a handful of big-name financial institutions—such as the former Fleet and Lehman Brothers—that went wireless and lived to talk about it, most of the industry still errs on the side of caution and bars wireless connectivity to corporate networks, says Celent analyst Jacob Jeger.

But as any parent knows, having rules about what's not allowed, and making sure

they're enforced when you're not looking, are two very different things. Sometimes the unauthorized wireless connections to the network are intentional, if not malicious—you can probably imagine a tech-savvy employee who wanted to use a laptop in a nearby conference room installing a wireless router from home and not considering the security vulnerabilities.

unlocked, you've created a vulnerability to be exploited," de Haaf adds.

Companies such as AirDefense, Network Chemistry, AirMagnet, Highwall Technologies, Newbury Networks and Fortress Technologies all offer products designed for continuous wireless intrusion protection being deployed by many financial institutions to enforce no-wireless policies. Most products require the installation of sensors on walls or in ceilings that constantly monitor and discover all the wireless devices in the environment. These systems continuously watch the behavior of all devices, on the lookout for any attempts to connect to the corporate network. If devices are determined to be



But other times the rogue connections are unknown even to the perpetrator. Network Chemistry product manager Brian de Haaff recalls a recent customer case: The bank's finance group purchased new LCD projectors with no idea that the seemingly simple devices had built-in IP access points. "They were broadcasting everything they were projecting—all the numbers—in an insecure way," de Haaff says. Air Defense has a similar example of a bank client that unwittingly installed 150 HP printers with built-in access points—nobody seemed to notice the little antenna on back until Air Defense was in house doing a wireless audit.

"It doesn't mean you meant harm, but if somebody comes pulling on all the front doors in the neighborhood and yours is

rogue, or even malicious, the enterprise-monitoring systems can take preemptive action to isolate the devices so that they can't transmit data.

AirDefense and Network Chemistry have a fairly sexy sales tool: mobile detection devices used to prowl for unauthorized wireless connections to the network, pinpointing locations within several feet.

AirDefense estimates that 30 percent of its customer base includes no-wireless enterprises that sign on for rogue protection, but "once they have control over their airspace, they're quickly willing to go into a [wireless] deployment because they feel safe," says David Thomas, vp of product management at AirDefense.

It may be some time before that rings true for financial services.