

Security

How Lehman Brothers Overcame Its Wireless Fears

David M. Ewalt, 03.17.05, 6:00 PM ET

If you think that wireless applications have become completely ubiquitous in corporate America, think again. Consider **Lehman Brothers**, a multibillion-dollar global company with 20,000 employees that, until last year, had a firm no-wireless policy.

The reason? "All the security issues," says Lehman (nyse: [LEH](#) - news - people) senior engineer **Fred Nwokobia**.

As wireless networks have proliferated throughout the world of enterprise computing, so have the threats to businesses' privacy, security, and efficiency. Companies around the world have already seen the benefits of unwiring their infrastructures, but now they're realizing that freedom comes with risk. In fact, as evidenced by Lehman's reticence to embrace wireless, security concerns may be inhibiting its growth.

To address those issues, some security providers are developing products specifically for wireless networks--sophisticated tools that scrutinize and supervise the airwaves. Products from companies like Atlanta-based **AirDefense** let businesses constantly and automatically check their networks for malicious activity.

"An essential part of any security strategy has to include monitoring the wireless airspace," says Forrester analyst Paul Stamp. "You need to look for both unauthorized activity by your employees, and in more critical areas you've got to be looking for that guy in the parking lot with an antenna."

Wireless security isn't a new issue. In the early days of Wi-Fi securing a network was mostly a matter of authentication and encryption; making sure you could identify your users, and that they weren't sending unprotected data over the airwaves.

Today, new methods of spying on wireless communications have made the job a lot tougher. Attacks like the "evil twin" disrupt a company's network from the outside, jamming its radio signals or bogging it down with a denial of service attack, then broadcasting a counterfeit signal into the building. Users struggling to get back online then re-connect to the spoofed access point, allowing the attacker to spy on their communications.

AirDefense's product, called Enterprise 6.0, can thwart such a breach. That's why Lehman in Jan. 2004 finally felt comfortable enough to install wireless access points. Today it has 500 installed worldwide.

The AirDefense system is generally run off of an **Intel** (nasdaq: [INTC](#) - news - people) based server installed inside a corporate network. Sensors out in the field monitor all the traffic area and report back to the box, and the software provides users with a real-time, graphical view of what's going on inside their network.

If a company already uses access points from other providers like **Cisco Systems** (nasdaq: [CSCO](#) - news - people) they can be configured to also serve as sensors; otherwise, AirDefense sells specialized hardware to do the job. Users see a mapped-out rendering of their office showing the strength and location of various access points, who's using them, how much traffic is in the air, and if any unauthorized nodes have popped up.

"I think of it like a police helicopter that's flying on top of a city," says **Jay Chaudhry**, AirDefense's founder. "We look at the flow of traffic, if it's flowing right, if it's slow, if it's moving at the wrong speed," he says.

Lehman's Nwokobia says these simple monitoring functions alone have already paid for the cost of deployment. "It's a great capacity management tool," he says. "I can see uncovered pockets of floor space and either put more APs (access points) there or boost the signal on existing ones."

But more importantly, this virtual traffic copter can also keep an eye out for network issues that are more troublesome, like unauthorized users and outside attackers. "You can see someone violating the speed limit,

you can see someone driving on the wrong side of the highway," says Chaudhry. "You can see people where they're not supposed to be."

Nwokobia got his first taste of the power of this real-time monitoring when the system first got up and running. Right away, he started seeing an outside device repeatedly trying to access his network. "It wasn't people attacking, it wasn't a fake access point...but we could tell there was this outside Symbol device," he says, referring to the company that makes handheld devices for supply chain management.

"We kept wondering how come at 3 P.M. every day, we saw this kind of activity." Eventually, he realized the problem was a regular visit from a wirelessly enabled **Sears** (nyse: [S](#) - [news](#) - [people](#)) truck, and the IT staff was able to relax its defenses.

If there is a real threat on the network, Nwokobia and his team can fix it remotely using the software, shutting down rogue access points or boosting the power of their own antennas to jam signals coming from the outside. That sort of remote access and granular look into suspicious activity simply wasn't available without AirDefense, says Nwokobia.

The system gives them so much intelligence that it spares IT workers countless hours investigating problems and traveling from their New Jersey data center into Lehman Brother's offices in New York's Times Square. "If we didn't have this visual representation, we'd be sending IT teams all around just to figure out what's going on," says Nwokobia. "It's saved us huge numbers of man hours just from moving around."

A typical Airdefense deployment starts with just one location, about ten access points, and one sensor, says Chaudhry, and costs under \$10,000. But over time, users tend to expand the system along with their wireless presence. They can also invest in other tools like AirDefense Personal, software which sits on a laptop computer and helps protect data when a worker is using his computer wirelessly while traveling.

AirDefense was the first vendor to come out with an enterprise solution for monitoring wireless space based on the ubiquitous 802.11 standard, says Forrester's Stamp. And he says **the company still has the most sophisticated product.**

That's a bold statement for a company that's barely four years old. Chaudhry founded AirDefense in 2001 after selling his previous company, SecureIT, to VeriSign (nasdaq: [VRSN](#) - [news](#) - [people](#)) for about \$70 million.

Its competitors, mostly private companies like AirMagnet, Aruba Networks and BlueSocket, are putting pressure on AirDefense, but they've yet to put a dent in its leadership position says Stamp. "They are facing increasing competition but there will always be a place for a more sophisticated security solution."

For now, Lehman Brothers isn't seeing much in the way of concerted, malicious attacks on its wireless network. But Nwokobia says he's confident he can handle it if it does happen. "If there is a crazy attack, we now have the ability to see it and do something about it," he says. "It's nice to know that the tools are there."