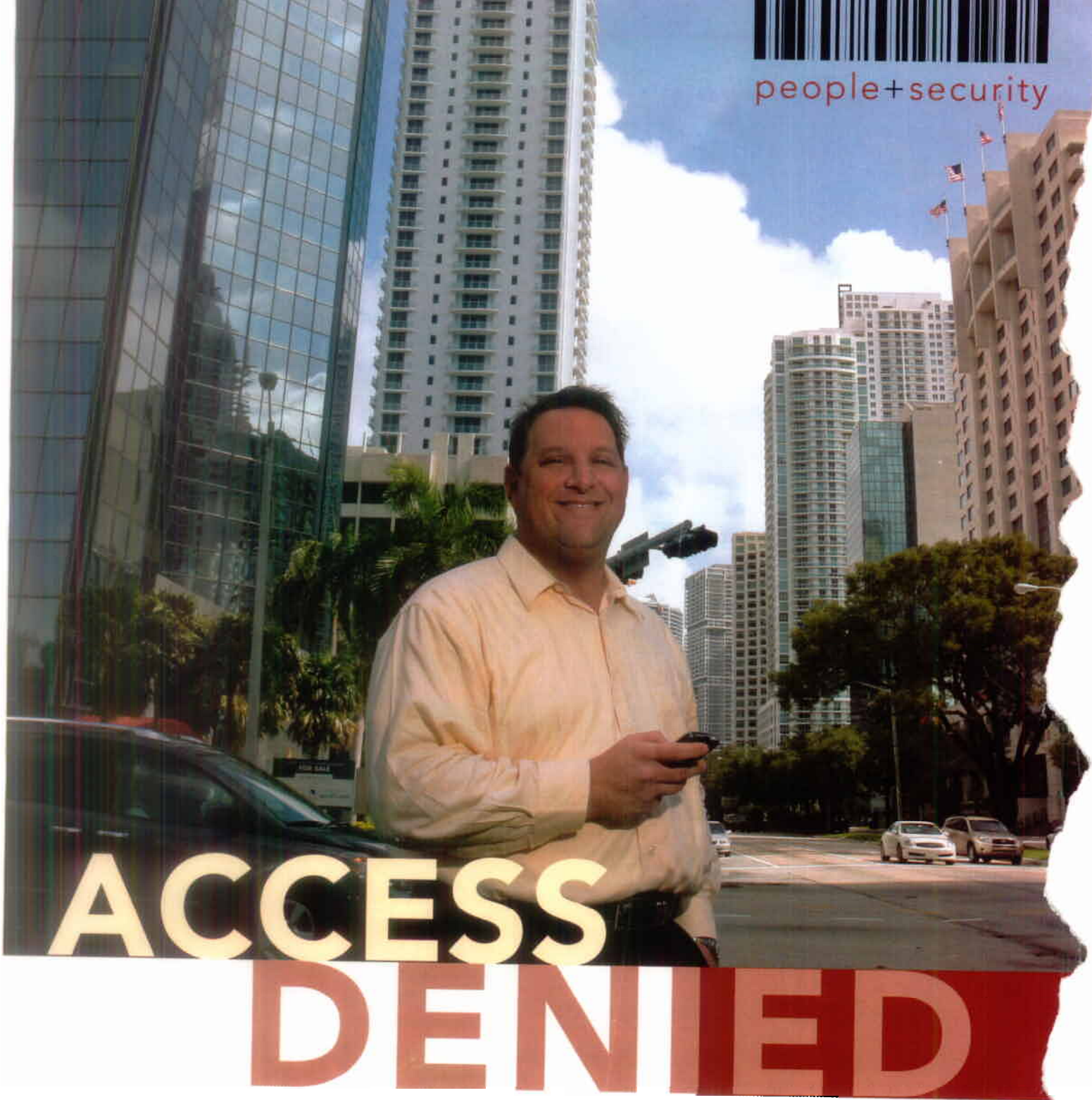




people+security



When managers at a Brickell area medical office realized that their network had been hacked and emails were being hijacked, they called Ilan Sredni.

“Our technicians were able to penetrate their wireless network in under eight minutes,” says the president of North Miami-based Palindrome Consulting, an IT security company. Among other issues undetected by existing software, Sredni’s techs found holes in the firewall that were leaking information to non-authorized parties.

It’s not a new crime, but computer hacking is a growing crime with serious repercussions for companies with unprotected wireless networks, says Sredni.

“Business owners do not realize how much they are at risk until it’s too late,” he warns. “Hackers are ever-changing malignant cells always looking for a point of entry.” Once inside, they can access every piece of information available to legitimate network users, including financial data, banking usernames and passwords, credit card numbers, employee social

security numbers and other sensitive information.

They can also access the Internet to commit cyber crimes such as uploading child pornography – a felony that law enforcement will trace right back to the unfortunate company with the unsecured network.

The most alarming aspect of the crime, says Sredni, is the ease with which it is accomplished. All it takes is a laptop computer, easily obtainable software, and a low-cost antenna capable of scanning for unsecured networks from a passing car.

To keep computer users informed about the potential perils of wireless systems, Palindrome hosts occasional workshops such as a free event on Dec. 11 featuring security experts from the FBI, NAP of the Americas and U.S. Attorney's Office.

Originally from Colombia, Sredni moved to Miami in 1981 and earned a degree in MIS from Florida International University in 1991. He was recruited by Pepsi Cola International as its integrated solutions projects leader for Latin America, and later joined the Protective Group as director of technology and operations manager in Colombia.

In 1996, he partnered with a friend to open an e-commerce site, while launching his consulting business. Three years later, he opened Palindrome Consulting as an IT support company, but shifted its focus to network security when he recognized a need within small- and medium-

information theft in the last nine months.”

He adds, however, that the NAP – a mammoth cyber gateway connecting the majority of Latin America and the Caribbean to more than 148 countries worldwide – has seen little to no increase in attempts to infiltrate its systems. Located downtown, the 750,000-square-foot data center makes Miami one of the five best-interconnected cities in the world, ahead of San Francisco, Chicago and Washington, D.C.

But while the NAP is manned by security personnel 24 hours a day, 365 days a year, the same cannot be said of many South Florida companies. “We find that while in-house IT staff and independent IT support companies focus on the day-to-day maintenance issues of a company's network, security often takes a back seat,” says Sredni.

“It's important to understand that the Internet allows anyone to

learn about hacking programs, expanding the pool of potential criminals daily,” states Sredni. “In addition, the boom in wireless connections greatly increased the vulnerability of systems to drive-by hackers.”

To help determine the safety of a wireless network, Sredni recommends that business managers ask themselves the following questions:

- Is the network monitored regularly?
- Are passwords sufficiently complex and changed often?
- Is anti-virus software current on all the machines and is it centrally monitored?
- Is employee-use of instant messaging protected from viruses and abuse?
- Are ports open on the company's network to the outside and why?

- Are tools in place to control access to certain web sites?
- Is laptop data encrypted to prevent unauthorized access in case of loss or theft?
- Are rogue access points or extensions to employee home systems accounted for and protected?
- Are all work stations and servers kept up-to-date with service packs and security patches?

“If the answers to these questions is no,” says Sredni, “the network is definitely vulnerable to hackers.”

Comments? Editor@miamimonthlymagazine.com

Business owners do not realize how much they are at risk until it's too late.

Ilan Sredni slams the door on wireless network hackers

sized businesses with limited resources. Over the last year, Palindrome has doubled its employees and increased monthly network security assessments fourfold, thanks to South Florida's emergence as a hotspot for hackers.

“Even though Miami does not have as large a technical base as Silicon Valley and New York City, it has become a high profile target due to its tourism, hospitality and international financial activity,” states Christopher Day, senior VP of secure information services for Terremark's Network Access Point of the Americas. “This has translated into a significant elevation in investigations on personal identity