Snoop Stopper

Published: Sunday, December 23, 2001 in the St. Paul Pioneer Press

BY MARTIN J. MOYLAN Pioneer Press

Cruising about the Twin Cities, with his wireless laptop on the seat next to him, Brad Rubin can see one business opportunity after another pop up on his computer screen.
His laptop, hooked to a homemade antenna housed in a Pringles can, runs sniffer software that detects wireless networks, even those people have tried to hide. Many are not protected by encryption, making it easy for someone with a wireless modem to plug into them and snoop -- or worse, Rubin says.

After nearly 20 years of working in the information technology arena in the corporate world, Rubin is trying to establish himself as an independent computer security consultant.

With all the concerns these days about data security and privacy, corporate espionage, cyber-vandalism and, possibly, cyber-terrorism, the outlook is good for the information security market, he expects. And he sees wireless security, in particular, as a solid foundation for a business.

"Wireless vulnerabilities have only recently started to receive national attention," he says.

Many businesses and consumers are connecting their computers with wireless networks. Especially popular are 802.11b (Wi-Fi) networks because they're easy to set up and use.

Yet many businesses and consumers don't turn on the encryption systems meant to thwart most snoops. Even when they do turn on built-in encryption programs, skilled hackers may quickly get past them.

"I can take a look from the outside, through the eyes of a cracker, for vulnerabilities," Rubin says. "When people get firewalls, they think they've done what they're supposed to do. But they're (often) not sure what they look like from the outside world."

On a recent half-hour drive around downtown St. Paul and Minneapolis, Rubin detected 24 wireless networks. Only 14 had encryption turned on.

In addition to advising companies about the deployment of new wireless network and security of existing ones, Rubin also sees opportunities in computer forensics, divining what has been done with computers and files produced on them.

Companies like to address some issues, such as the theft of trade secrets, quietly, he notes. And police generally don't make investigation of white-collar crimes a priority.

"Computers are increasingly used in crimes, and companies need someone they can turn to other than law enforcement," he says.

Rubin says his experience in the corporate world prepared him well for his career change.

For 15 years, he worked for IBM in Rochester, focusing on projects involving IBM's AS/400 servers. He

also led the development of a major IBM Java software program. For the past three years, he was chief technology officer for Imation data storage division and led its R&D team.

"I wanted to take what I've learned about technology, marketing and sales and combine it," he says. "Now, I get to explore fun stuff like this (ferreting out vulnerable wireless networks) and turn it into money."

His part-time teaching job at the University of Minnesota's Institute of Technology and his children, ages 8 and 11, also make work flexibility and minimal travel important. With Imation, he was often on the road.

His biggest challenge is getting potential employers to notice him.

"I have to try to communicate the services I offer and the capabilities I have to the right decision-makers in the Twin Cities -- without a big marketing budget," he says.

He does have the prerequisite Web site (http://www.bradrubin.com/). In his first three months as a consultant, he's landed several jobs through the Gerson Lehrman Group, which matches IT consultants with mutual fund firms.

Companies with and without their own IT staff would find it worthwhile to have outside eyes cast on their computer security efforts, Rubin says. That's evident from all the open wireless networks he's finding.

"For companies that outsource their IT, it's even more important that they verify they're getting appropriate security," he says.

He sees most of his competition coming from consulting firms, such as Anderson Consulting, which have security practices. He figures he can undercut their prices. But he won't rule out partnerships with them.

He knows many execs at those consulting firms through his work at IBM and Imation.

Rubin managed his savings and investments so that he can take some time to establish himself as a consultant.

"A lot of people start out undercapitalized and don't pay attention to keeping new business in the pipeline," he says. "A lot of consultants market themselves too broadly. Instead of being very clear and specific about the services they offer, which tends to get better results, they market themselves as jacks-of-all-trades. My goal is to have the greatest expertise in wireless security in the Twin Cities. And I'm giving myself one year to achieve success."

Martin J. Moylan can be reached at mmoylan@pioneerpress.com or (651) 228-5479.