Stopping wireless ID theft

September 16 2005

A New Jersey State Superior Court judge this week ordered a company that had acquired customer names from a major wireless carrier without its permission to refrain from selling those customer profiles to others and to surrender the names and transaction records.

The order in the case of Verizon Wireless vs. Source Resources Inc. is the latest round in the ongoing war centered on stopping ID theft today, experts told UPI's Wireless World.

"Accessing a person's personal telephone records without a valid court order or the customer's permission is illegal," said Steven Zipperstein, general counsel of Verizon Wireless, in Bedminster, N.J. "We will use every weapon in our legal arsenal to shut down identity theft operations."

Many other wireless and IT experts, however, said the legal approach should be the last resort, after other internal options have been exhausted to protect confidential customer data.

"Much of the data compromised has been due to hacking and poor security measures," said Robert Siciliano, a personal-security and ID-theft expert in Boston, whose clients include British Petroleum, among others. "Government intervention is making corporations liable, through a variety of new compliance and regulatory standards."

Siciliano also noted that internal networks are what are being breached today by insiders, as external hackers are being kept away by firewalls and other technology measures.

"Hacking from outside is becoming more difficult," Siciliano said. "Monitoring of internal networks through a variety of platforms is a priority to reduce employees theft. Knowing who's accessing what and why is essential."

Other experts agreed, but added technology alone is not the answer.

"Many companies do a horrible job in protecting customer's private information, actually all information," said Ted Demopoulos, an IT consultant and author of a forthcoming book from Dearborn Trade Publishing. "Technologies like strong authentication, encrypted backups, appropriate authorization, can help, but technology alone is no solution."

Rather, he said, companies need to develop a written plan, a security policy. Then they need to brief everyone in the firm on the plan -- and make sure that they follow it. The plan should specify rules to protect customer data and should categorize information into secret, confidential, restricted or public categories. These policies also restrict where customer information can be stored.

For example, it may prohibit customer data, names, addresses and Social Security numbers from being stored on laptop computers.

"Without a workable data security plan, information security for private customer data will be hit or miss," Demopoulos said.

In the Verizon case, all that is being said is that Source Resources, of Cookeville, Tenn., obtained the customer data without permission. It is not being publicized how the information was acquired. Superior Court Judge Harriet Derman this week ordered a "permanent injunction" against the company, which has agreed to return all the records to Verizon, as well as information about "how it obtained customer records."

The lawsuit was filed July 8 after Source Resources advertised on its Internet site that it had the ability to find confidential wireless phone numbers for a fee. One of Verizon's own customers reported that his private phone records allegedly had been obtained by Source Resources, and that prompted the lawsuit by Verizon, which has more than 47 million customers in the United States.

Private companies, such as Verizon or Morgan Stanley, however, are not the only ones whose data is being stolen. The Pentagon recently reportedly suffered a security breach by foreign governments.

The consulting firm Guidance Software worked with the Department of Defense to "uncover hacking incidents on the department's massive network, but detect, track and extinguish active hacks that lived on the network, which were previously unknown, and that searched for classified information and sent that information out, daily, to secret repositories," said a spokesman for the company, a cyber forensics firm, based in Pasenda, Calif.