SILICON VALLEY / SAN JOSE
Business Journal

DECEMBER 30, 2005
VOL. 23, NO. 28

96 N. Third St.
Suite 100
San Jose, CA 95112

Protecting against digital data thefts with a 'kill switch'

BY TIMOTHY ROBERTS
troberts@bizjournals.com

DENNIS G. HENDRICKS

LOCK FOR WAYWARD LAPTOPS: Jim Obot, left, president and CEO of Beachhead Solutions Inc., and Tim Lavelle, vice president of sales, say their company has created a "killer app" for laptops that will thwart data thieves.

The latest weapon in the war against data theft is a killer app.

The company's founder uses words like 'kill' and 'self-destruct' to describe what his product will do to a wayward laptop, all in the name of keeping data from falling into the wrong hands.

Beachhead Solutions Inc., a Santa Clara-based startup, is offering a software program that allows a company's IT director to instruct a laptop to begin overwriting all of its data — several times over just to make sure.

Even if the laptop isn't reported stolen, the software will order up the self-destruct option when the computer hasn't signed onto the network for a set period of time.

"What we've done is to put control in the hands of the owner and took it away from the user," says Jim Obot, Beachhead's president and CEO.

With an increasing number of reported thefts of customer information from financial institutions, many security-conscious executives have been looking for ways to take control of the data that rides around under the arm of peripatetic sales and engineering staff members.

The pressure is even greater for companies doing business with California, which requires companies to notify customers of data theft.

The idea for the Beachhead Lost Data Destruction 1.0 came about in discussions that Mr. Obot had with the U.S. Army. The military is concerned about the security of data in laptops carried in Humvees in Afghanistan and Iraq. Commanders wanted to know if there was some way to order the destruction of the information on hard drives that fell into enemy hands.

"Blow away all my data?" asked Tim Lavelle, vice president of sales. "We hadn't thought of that before."

Destroying data with "a go-kill-yourself message" has been in use for hand-held devices like PDAs and smart phones, says Eric Maiwald, senior analyst for the Burton Group, a computer security firm. But to apply that to a PC is something new, he says.

There are three ways to trigger the data destruction:

- An employee calls IT and says his or her laptop has been stolen.
- The laptop fails to connect to the network for a long period of time. Then, when it is finally detected by the server, it will receive the overwrite message.
- The network detects repeated attempts to sign in with the wrong password.

Mr. Obot admits that potential customers sometimes blanch when they hear "data destruction." He promises a partnership in 2006 with a company he won't yet name that will add data backup and recovery to Beachhead's Lost Data Destruction suite.

Reassurance that data will be regularly backed up will give users greater confidence in using the tightest security boundaries, Mr. Obot says.

A really advanced data thief might try to pull the hard drive out of the laptop to bypass the kill command. But on a computer protected by Beachhead, the thief will find that the data is further protected by encryption.

Beachhead started in 2003 with money from friends and angel investors, Mr. Obot says. It has operated so far on $4 million to $6 million. It has 20 employees and sells mainly though partners, reducing the need for a large sales staff. He promises more partnerships in 2006.

Heritage Bank of Commerce of San Jose, one of Beachhead's first customers, has a policy of not storing data on office computers, but Larry St. Regis, senior vice president of information services, says, "Our policy is only as good as the people who read and make use of it. We wanted to make sure that there was no way that anyone could break the policy or accidentally store something sensitive on a laptop."

So far Heritage Bank hasn't had to call rewrite, but a tax auditor from Mohler, Nixon & Williams, a certified public accounting firm in Palo Alto, did make use of the feature. A thief took a laptop from the trunk of an auditor's car while it was parked in San Jose. The auditor reported it lost, and the Beachhead system went to work, overwiting all the data.

Mr. Obot says he knows the system worked. The computer checked in with the systems administrator, he says, and announced that data destruction had begun.

TIMOTHY ROBERTS covers public policy, corporate governance and Internet security for the Business Journal. Reach him at (408) 299-1821.