

Internet & Technology

SECURITY SOFTWARE

Israeli Security Firm Replaces Vaults With Cyber Safes

By Donna Howell
Investor's Business Daily

The Israeli arm of consultant Deloitte Touche Tohmatsu had a problem to solve. Employees had to run all over, even as far away as Turkey, to pick up confidential documents from clients. Then those papers had to be kept in a safe.

It amounted to a ton of inconvenience. But heavy security is a must in order to do work for some clients, like defense contractors.

"They came to check on us," said Eyal Assayag, manager of computer risk services. Clients wanted to know how well their information was being guarded. They'd ask things like, "Did we put it in the right place, are procedures okay?" Assayag said.

Deloitte & Touche-Brightman Almagor & Co. — as the Israeli practice is formally known — also does work in Israel's competitive mobile phone industry. That, too, warrants locked vaults, Assayag says. An accounting project, for instance, might require storing sensitive salary data.

"When you say 'Israel' you say 'security,'" he said. "We have all these problems here, and some of our clients are very sensitive about their information."

Deloitte's Israeli practice, based in Tel Aviv, did use a safe. But it was awkward to do so. Several times a month, workers traveled to get client documents that couldn't be entrusted to anyone else.

In search of a better way to handle data, the firm turned to an Israeli security company for help. Cyber-Ark

Software Ltd. in Tel Aviv didn't do away with Deloitte's locked safe. It just moved it onto the computer network.

Using Cyber-Ark's virtual safe helped the consultancy cut the hassle of using a real vault. It trimmed man-hours that workers spent fetching papers, and made data-trading with clients easier, Assayag says.

Narrowly Focused Approach

Cyber-Ark, which opened U.S. headquarters in Dedham, Mass., in December 2000, takes a targeted approach to security. It doesn't try to keep whole networks safe. Instead, users put sensitive data into a kind of online vault. They click on a computer icon of a safe, then type in passwords to enter.

The safe is built within software that runs on a dedicated server and has built-in security. A firewall deflects hackers, and a strict access control feature keeps a short list of who's allowed in.

Also built in is a virtual private network, which allows access to the vault securely over the Internet. All data in the vault is encrypted, and can only be unscrambled by authorized users.

"Using the Web is a very, very good feature of the software," Assayag said. "We don't have to send anybody (to get sensitive information) anymore — we encrypt it on the Web."

About five Deloitte clients are now using the Internet to share data securely with consultants. "Using the vault over the Web, we have the opportunity to open a safe for each of our clients," said Assayag. Each client has a different "safe" in the system, of course.

Clients can see documents that have been put into the vault, and add new ones. "Data is protected while it resides in the vault, while it's transmitted over the Internet and while it's used by the end user," said Orit Rumstein. She's vice president of

international marketing for Cyber-Ark. The firm's roots are in defense. Co-founder Alon Cohen handled computer security for Israel's military, and advised security companies.

"Alon was auditing large banks for their (computer) security and always found holes. It was almost inevitable," said Chief Operating Officer and co-founder Udi Mokady. Cohen wanted to make banks' networks operate more like traditional bank security.

In the physical world, banks "don't try to protect the entire building, they try to create one very secure location," said Mokady. So Cohen began developing a computer security system that would work the same way. It would look like a real bank right down to the icons of vaults where sensitive data would be stored.

No Experts Needed

"He wanted a solution that wouldn't require expertise to use," said Mokady. "A safe for data is something you immediately recognize the need for."

The visual theme is carried further. "A yellow dot on a safe indicates someone other than you accessed this safe," Mokady said. A green dot means a new object and a blue dot means a file was retrieved.

Such easy-to-read cues are needed so clients can prevent abuse of their data, he says.

For instance, what if a lawyer leaves his firm and spirits away papers from all the cases he's worked on? "If you do that and have our product, you'll see those multiple files in blue," Mokady said.

About 25 organizations in the U.S. and Israel are using Cyber-Ark's product. The company is now working on ways to deliver its software over a dedicated device. "It seems customers really like the idea of an appliance," said Rumstein, vice president of international marketing. "All you have to do is turn it on and plug it into the network."

