

VANCOUVER BUSINESS JOURNAL

Key to Southwest Washington Business

SECURITY *TO GO*

CRU-DataPort designs and manufactures removable hard drive enclosures – military and government agencies are longtime customers

BY SHANE CLEVELAND

VBJ Staff Reporter

The U.S. Northern Command was created in 2002 to provide command and control of Department of Defense homeland security efforts and to coordinate military support to civil authorities. NORTHCOM is based out of Peterson Air Force Base in Colorado Springs, Colo., and is staffed by about 2,000 civilian and military personnel. The thousands of computers manned by NORTHCOM's staff contain information critical to performing their duties and must be kept out of the wrong hands.

A Vancouver company plays a significant role in protecting information stored on NORTHCOM's computers.

CRU-DataPort manufactures removable hard drive enclosures designed to provide data security and mobility to its users like NORTHCOM and other government agencies and private-sector companies. NORTHCOM can remove hard drives from computers and securely store them, such as in a safe. In an emergency, hard drives can be removed and taken to an

alternate location, giving staff instant access to stored information.

Data security awareness has increased since the terrorist attacks of Sept. 11 and amidst growing concerns of computer crimes and identity theft. And CRU-DataPort has tailored its product line to meet the demand.

"The goal is to make it so everyone in every market can make their drive removable," said Jon Johnson, CRU executive director of marketing.

CRU-DataPort was founded in California in 1986. In 1999 it was bought by Vancouver-based Labtec Inc. and moved to Labtec's headquarters in the Columbia Tech Center. Then in 2001, CRU-DataPort became a subsidiary of Logitech when the publicly traded company acquired Labtec. In 2002 the company went full circle and once again became independently owned following its buyout by a Portland-based acquisition group. Randal Barber, who helped facilitate the transaction, became CRU's president and CEO, and the company moved to its own building in Columbia Tech Center.

The company operates in 16,000 square feet of office



and warehouse space in the Tech Center. CRU's approximately 40 employees engineer, design, assemble and market its products from its Vancouver facility. According to Johnson, the company's founders were involved with the military, and the idea for the product was derived from the need to secure computers on a military base. Entire computer towers had to be hauled into secure storage spaces when all that needed to be protected were the hard drives. The resulting solution was a removable enclosure for computer hard drives, and the adoption of the product by government and military was rapid, said Johnson.

The original DataPort 1 was used in a space shuttle.

Its product line has grown to serve several markets. Prices range from about \$20 for its affordable consumer model to more than \$60 for its professional models. The enclosures are designed to fit into factory computer towers and are compatible with PCs

and
Mac s .

CRU has partnered with manufacturers such as Dell and Gateway to customize DataPorts to fit the distinctive designs of their products. Once installed, the drives can be key-locked into place to prevent just anyone from removing the hard drives. Its line includes an external HotDock that connects to a desktop or laptop through USB or FireWire, allowing multiple hard drives to run simultaneously or be swapped out. CRU's Encryption DataPort offers military-grade data protection for a computer's hard drive. Even if a hard drive is stolen, a security key unique to each enclosure must be used to access data on the hard drive. Adding encryption was a natural extension for the company.

"Our market focus is in data security and data mobility," said Johnson. "To make data mobile, you want to make it secure."

This varying multitude of features has allowed CRU to target several markets.

Regulations stand to broaden customer base

"When you find out your hard drive is removable, you find there are a lot of applications for it," said Johnson.

The same security and mobility features attractive to the military and government agencies could be of use in the corporate world, as evidenced by recent breaches. Just last year, companies such as Wells Fargo, Ford Motor Co. and H&R Block had computers with information about customers and employees stolen. Johnson said protecting the information through encryption or removing hard drives to a more secure location can prevent such losses. Using a DataPort as a second hard

drive in an expansion bay or external enclosure allows a user to backup computer files on the fly. In the case of a disaster or system failure, a business' information can easily be retrieved.

The mobility feature has proven beneficial to organizations such as universities as an affordable way to increase efficiencies and flexibility of classrooms and equipment. The removable drives allow hard drives to be easily swapped between offices and classrooms.

Portland business consultant Sheldon Penner has worked with CRU-DataPort for about three years. His



Submitted photos

Removable hard drives can be used to back up information or to hide it from potential thieves.

firm, Amicus Data, specializes in data back-up, storage and recovery for businesses. Penner said he recommends CRU's products for customers seeking data back-up and security solutions. Some of

his clients have had bad experiences with removable drives in the past that were cheaply made.

"Small business customers can be very finicky," said Penner. "In the end they just want it to work."

CRU-DataPort has been focused on recapturing market share lost after its product patents expired and competition grew.

"Growth has been steady," said Johnson, "because we have been targeting growth in different categories in addition to maintaining our focus on where our strengths lie."

Its move back to a privately held company has allowed it to adapt to the market and focus on product development and customer service, said Johnson.

"Getting out there and regaining our competitive positioning is how we started that growth process. Since then, it has been a formula of maintaining our presence in traditional strongholds and also slowly growing into the areas that it really makes sense," he said.

The company expects steady growth, particularly as state and federal legislation begins to mandate greater levels of security and protection of data.

MISSING IN ACTION

Thieves are finding more value today in the information stored on computers than the hardware itself. Businesses across many industries are vulnerable because of the information they collect and keep regarding employees and customers. CRU-DataPort realized simply removing a hard drive did not prevent information from being stolen from it. The company's Encryption DataPort protects data placed on the drive and requires a security key to access it. Similar technology could have prevented loss of information by companies in the past, which opens up employees and customers to identity theft and mars the businesses' reputation.

FEBRUARY 2005

Bank of America lost backup tapes containing data on 1.2 million credit card holders.

MARCH 2005

A computer stolen from the Nevada Department of Motor Vehicles held information on more than 8,000 people.

APRIL 2005

Ameritrade lost backup tapes containing data on 200,000 customers.

JUNE 2005

CitiFinancial lost backup tapes containing data on 3.9 million people.

NOVEMBER 2005

A stolen laptop contained HR data, including social security numbers and bank account information on 160,000 Boeing employees.

DECEMBER 2005

The Ford Motor Co. had computers stolen that contained sensitive information of 70,000 current and former employees.

JANUARY 2006

Providence Home Services in Oregon had data stolen containing information on 365,000 patients.

MARCH 2006

A laptop was stolen from Fidelity Investments with information on 196,000 retirement account customers.