

# “YOU CAN’T HACK WHAT’S NOT THERE”

AN UNWAVERING FOCUS ON PROVIDING CUSTOMERS WITH RELIABLE AND CONVENIENT WAYS TO SECURE, BACKUP AND TRANSPORT DATA HAS MADE DATAPORT THE RECOGNIZED DE FACTO STANDARD FOR REMOVABLE HARD DRIVE ENCLOSURES. IWA SPOKE WITH CRU-DATAPORT’S JON JOHNSON ABOUT GETTING TO THE TOP – AND STAYING THERE.

**C**RU-DataPort has been developing data security and storage devices for computer systems since 1986. DataPorts are used by many government agencies and are designed into Classified Networks, Secure Workstations, Forensic Computers, Rugged, Tempest and Zoned PC’s worldwide.

“DataPorts make any standard 3.5” or 2.5” disk drive removable for security, backup, PC-sharing and data archiving purposes,” says Jon Johnson, Director of Sales and Marketing for the company. “With well over 2,000,000 units installed in computer chassis, rackmount systems and custom enclosures worldwide, DataPorts are a proven solution for removing, hot-swapping and protecting your data. DataPorts are rated for 25,000 insertions, include lifetime toll-free support and are backed by the industry’s leading 10-year warranty.”

**IWA.** CRU-DataPort has been involved in security for quite some time. How has the market changed in the last few years? What are the main reasons for these changes?

**JJ.** The data security market has changed significantly over the last few years with 9/11 and its after-effects being the most significant factor for many of these changes. For most organizations, data security might have been somewhere in the top five IT spending categories since before Y2K. But in the post 9/11 world, increased awareness and budget for data security have made it a top priority for many in both the public and private sector.

As a result, the War on Terrorism, the USA Patriot Act and the President’s initiative to secure cyberspace are driving many of the changes we see in the security market today. The Department of Justice and other agencies are continually working to prevent computer crimes and enforce existing laws to keep cyberspace safe for all Americans, which includes protecting the intellectual property rights of our nation’s inventors and creators. Other government initiatives have led to significant changes in security including the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLB). Both are designed to among other things help secure the growing stockpiles of data being collected on individuals. With identity theft being the number 1 crime in America today, this is another main reason for the changes we’re seeing.

In addition, at no other time in the history of IT has protecting information from viruses, worms, Trojan horses and hackers been as critical. Cyber attacks are growing ever more sophisticated, programmed to unleash digital assaults aimed at specific entities and at pre-determined times. The most recent examples we’ve seen were designed to avoid federal and military users, but one can only expect that it’s a matter of time before future ‘malware’, or harm-causing software, will target vulnerabilities in our nations infrastructure, commercial or otherwise, increasing the necessity to improve our defenses against them.

As internet threats become more difficult to deal with, network security concerns are compounded by the continuous introduction of new hardware and software technology, such as wireless LANs, which introduce the potential for unanticipated breach points. Furthermore, security planning today cannot focus only on prevention of external attacks, but must also avert security violations from within the agency or enterprise, where data theft from employees or insiders can be even more difficult to deter.

As a result, the job of today’s CIO is increasingly complex and the expectations on them continue to rise. They must not only keep up with these changes in technology, but do so in a continuous and collaborative fashion, while merging new solutions with legacy systems and fast enough so the technology isn’t outdated before the ROI can be realized. For government CIO’s the task is even tougher as literally thousands of vendors are competing for existing as well as newly emerging Federal program funds.

The security market is dynamic with many changes in store for years to come. These changes affect us all so we must work together to address this growing concern. The President’s initiative to secure cyberspace identifies steps we can take, from Federal, state and local governments to private companies, organizations and individuals. We at CRU-DataPort are committed to do our part and invite others to join us in sharing concerns, ideas and creating new solutions.

**IWA.** Computer-based terrorist threats and perceived infrastructure vulnerabilities are driving security in the private sector and federal government. How do CRU-DataPort’s products meet these challenges?

**JJ.** The vulnerabilities are real, no matter how sophisticated we think our defenses are. Whether we're a government entity, a global corporation or a private citizen, it would be unwise to think we're immune from computer-based threats ranging from someone illegally accessing our private computer networks to cyber-fraud like the infamous Nigerian e-mail scam.

CRU-DataPort is helping to meet these challenges with several easy-to-use but difficult to exploit solutions. First of all, if you have sensitive data and don't want others to access it (e.g. classified data or patient information under HIPAA regulations) a DataPort can easily make the hard disk drive storing that data removable. DataPort's are rugged enough to withstand frequent use and are designed to protect your drive during transportation. For true physical security, we recommend taking that data offline, because as we say, "you can't hack what's not there."

Another challenge DataPorts help address is the 'grab it and go' scenario. If there's an emergency of any kind, within seconds you can take massive amounts of vital data with you. With the increasing capacity of today's storage devices, it's now possible to quickly secure entire networks, not just a stack of files. This can be important for anyone from agencies deployed overseas to the private user who may be faced with the need to leave their home unexpectedly at a moment's notice. Having your important information stored on a DataPort just makes good sense.

Yet another security need DataPorts help to address in both the private sector as well as the federal government is the need for redundancy (backup) and disaster recovery. The fastest way to backup the contents of a disk drive is to copy it to another disk drive. Putting a DataPort in your PC's expansion bay or using one of our new DataPortable external USB and FireWire enclosures, allows you to quickly backup important data from your primary drive and retrieve it later in case of a system failure. This is also an effective tool for archiving large amounts of data such as media files or database information.

DataPorts can also be used for Emergency Operations Center (EOC) readiness, allowing an IT team to setup a new network onsite much faster than before. DataPorts with preconfigured drives can be installed into the standard systems already in the field such as training labs, classrooms or administrative PC's. This compatibility allows any system to be quickly transformed from peacetime use to a more critical mission whenever necessary.

For even further data protection, we offer a new line of Encryption DataPorts, which will protect the data on your drive even if the entire PC is stolen. We offer standard DES and TDES (Triple DES) data encryption in a hardware based solution so the encryption/decryption algorithm runs in real-time with no load on the system. These new DataPorts completely encrypt all data going to the drive, including the file allocation table and virtual memory. We use a Triple DES cryptographic engine, which has been certified by NIST and CSE. To make deployment easier for current DataPort



**Another challenge DataPorts help address is the 'grab it and go' scenario. If there's an emergency of any kind, within seconds you can take massive amounts of vital data with you**



customers, the new encryption products are compatible with our popular DataPort V and V plus product lines, so all they have to purchase are new Encryption DataPort hard drive carriers. This is also a benefit for new customers who want to swap between both encrypted and non-encrypted DataPort hard drive carriers.

We frequently see examples of how DataPort solutions can prevent security issues. Last year computers were stolen from a firm in Arizona with hard drives containing the medical records and Social Security Numbers of 175,000 military personnel and their families. A similar theft occurred here in the Pacific Northwest just recently, where several laptops containing information on active investigations were taken from a local law enforcement office. A couple of months ago, Wells Fargo reported the theft of computers containing thousands of mortgage customers data and last September in Canada, computers containing private information on 120,000 individuals were stolen from a Revenue office in what could be the biggest loss of personal information in Canadian history.

The wealth of personal data stored on computers makes them a prime target when thieves break into any business or home. Any one of these computers could have been easily and inexpensively outfitted with a DataPort or used a DataPortable to remove and secure the stolen personal information. Further, an encrypted DataPort would have provided the latest in military level security.

CRU-DataPort products help America and our allies meet other crucial IT requirements as agencies strive to build bridges to one another. DataPorts allow authorized users to quickly access and share gathered intelligence, while making transporting that data much easier and in a secure fashion.

Because DataPort solutions conform to common expansion bay standards and support the latest data interfaces, they can be seamlessly implemented into many agencies' existing IT systems. DataPort solutions are also designed in a forward-thinking fashion so they won't become outdated soon after they're deployed. DataPorts are commercial-off-the-shelf (COTS) solutions and CRU offers the industry's leading warranty of 10-years because we understand the importance of reliability when it comes to your data and we stand behind our products 100%.

**IWA. According to a company statement, your engineering design team and support staff can "work with customers to develop solutions that meet their particular needs." Can you give us an example of this?**

**JJ.** Yes, I can give you several. First, we were the first to offer a removable hard drive solution that supported the SATA interface standard. This was due to significant interest from many partners. Second, due to customer requests we've customized DataPorts to fit the distinctive chassis designs of several major system manufacturers including Dell, Gateway and MPC. Third, we also offer narrow versions (142mm faceplates) of most DataPorts because several custom PC builders also have unique industrial designs, and require a narrower bezel to meet their customer's requirements for a removable drive.

Also, in response to the growing demand for more storage in less space, we're launching two new DataPort products this spring. Our new Small Form Factor DataPort 25 makes up to two 2.5" hard drives removable from only a standard 3.5" floppy drive bay. Our rugged stainless steel design is ideal for harsh environments and can be set up to run RAID 0, 1 and 0+1 (mirroring, striping and a mirrored stripe). The second product really driven by customer demand is our new Low Profile DataPort LP, designed to make any standard 3.5" hard drive removable while taking up only a small amount of additional space. It minimizes the required dimensions for housing hot-swappable storage devices in custom rackmount and multi-drive applications.

CRU-DataPort is a customer-driven solution manufacturer. While our engineering team is constantly looking for new ways to improve data security and data flexibility, we're always open to feedback from our customers and in fact, we invite it.

**IWA. You have described your solutions as 'many uses – one device'. What other significant uses does a DataPort have?**

**JJ.** Besides making a hard drive removable for security, backup and data archiving purposes, a DataPort provides several other benefits:

Schools and university's can easily switch from one curriculum to another by simply hot swapping the drives. Students can be issued their own DataPort HDD Carrier at the beginning of each quarter to manage their own files. This drastically reduces IT costs and increases data flexibility options for both the staff and students.

DataPorts are also being used for numerous multimedia applications such as video surveillance, movies on demand and video editing/archiving. Our robust connector technology enables real-time data transfer/playback which is essential for video, while our rugged enclosure design protects that data during transportation and storage.

Consumers are using our new line of removable drive solutions called PrivatePC which allows several members of a family to share a common PC but keep their private files secure. Each family member can have their own PrivatePC hard drive carrier to store their own files. This also helps eliminate what we refer to as 'kid clutter' and keeps other annoyances away from your important data.

DataPorts also enable switching between different native operating systems, languages and applications such as job-sharing. A removable drive also simplifies PC maintenance, allowing you to easily remove a drive to take to the store for repairs while the computer stays home where it can still be used.

There are very unique custom applications using DataPorts as well. DataPorts are used in 'Fast Lane' toll booths where data transfer speed is a must, because drivers don't stop and the data from a vehicles electronic pass must be captured quickly and then stored. DataPorts are also used in flight simulation modules where massive amounts of graphical content must be stored and accessed in real-time.

With the added flexibility of a removable hard drive and the need to quickly store, archive and access large amounts of data, our customers are finding new uses for DataPort solutions all the time, making them truly a 'many uses... one device.'

**IWA. CRU-DataPort recently previewed DataPort for secure ID cards. How does this work, and what uses do you predict within the homeland security arena?**

**JJ.** This is another example of how our engineering design team worked quickly to respond to a customer's demand for a unique solution. We were approached by a solution provider who wanted us to put a Common Access Card (CAC) reader into a DataPort so it could be removed from a PC chassis or rackmount system. The idea is pretty simple, where if the user authentication device was removed from the system or server, this would add another layer of security to the system.

Due to the effort the DoD and others have put into this technology and the potential for large organizations in all sectors to deploy this application for network and plant access, we saw this as another potential for a new DataPort solution. ■

Jon Johnson is Director of Sales and Marketing for CRU-DataPort. Jon has been responsible for CRU-DataPort's sales and marketing worldwide for over four years. He joined CRU in 1999 and was named Director of Sales and Marketing in 2000. With over 16 years of sales and marketing experience primarily in high-tech, Jon has worked at companies such as IBM Corp., Labtec, Inc., nth degree software and Creative Multimedia Corp. Jon holds a bachelor's degree in Marketing from Portland State University.