

**A**t no other time in the history of IT has protecting data from hackers, thieves and viruses been as critical. Malware attacks and computer theft are increasing at an alarming rate, while new regulations designed to protect sensitive information (personal, medical, financial) make data security an even greater priority. As cyber attacks and computer thefts grow more sophisticated, so must our defences against them. In addition to outside threats, security planners must also focus within, where data theft from employees or insiders is difficult to deter. Today, CIOs are looking for data security solutions that make use of advancing technology, integrate with legacy systems and are scalable yet affordable.

*DCI Corporation/  
Cordsen Engineering GmbH*  
**Keeping Sensitive "Data"  
Out of the Wrong Hands**

*CRU-DataPort™ Secures Data  
with Proven Encryption Technology*



*Encryption DataPort by CRU*

To address this need, CRU-DataPort, makers of the original DataPort removable hard drive enclosure used in classified networks, secure workstations, temper and zoned PCs worldwide, offer a new line of encryption DataPorts, designed to protect the entire contents of a hard drive even if the PC is stolen.

Encryption DataPorts feature the same rugged aluminium alloy design, gold-plated connectors and cooling features as standard DataPorts, which enable frequent removal and replacement of hard drives from a PC to secure data offline and protect drives during transport. New Encryption DataPorts also include a high-speed ASIC that encrypts all data before being stored on the disk drive, including the file allocation table and virtual memory. This processor uses a unique electronic key during the encryption process so encrypted data cannot be accessed without having both the same electronic key and the Encryption DataPort assembly. Keys can be used in multiple locations or shipped separately from the encrypted drive; ensuring data are not compromised during transport.

Certification of unique keys is assured based on random number generation software and CRU-DataPorts key management procedures. The encryption database is tested for randomness per FIPS 140-2 requirements prior to programming master keys. There is no "backdoor" to this system and CRU-DataPort does not maintain any key log. The encryption key is "tied" to the actual data on the disk, while the DataPort and encryption engine are "generic" to the process, allowing you to move encrypted data securely from one PC to another.

Both the National Institute of Standards and Technology (NIST) and Communications Security Establishment (CSE) have certified the cryptographic engine. Compared to software encryption which uses system resources and negatively affects performance, the hardware-based engine encrypts/decrypts data in real-time without using precious system resources and offers data transfer performance equal to a non-encrypted ATA/133 system.

CRU-DataPort offers different strengths of encryption from DES to TDES (Triple DES) and several customisable key management options to meet the highest-level security requirements. Encryption DataPorts are compatible with any operating system that supports IDE hard drives and install easily into any standard 5.25" drive bay (PC or MAC). Existing DataPort V and V plus users can use Encrypted DataPort drive carriers to switch between encrypted and regular data.

Encrypted DataPorts are cost effective, easy to use and prevent unauthorised access to sensitive data whether they are online, offline or on the move.

At the 2nd European Infantry Seminar the CRU-DataPort is exhibited at booth E6 of Cordsen Engineering. Cordsen are the European distributors of DCI Corporation, which – in turn – is the global authorised distributor for CRU-DataPort.

For details about Cordsen, please see the marketing report on "Rugged Windows PDA" in this issue. For details about DCI Corporation please visit [www.dci-corp.com](http://www.dci-corp.com)