

Making Sure Resting Data is All Tucked In

April 2007



ON CYBER PATROL



Mobile computing technology advances gives us unprecedented flexibility in completing our mission both in combat, training, and our daily duties. One of the key components of this is the ability to store large amounts of data on laptops and in small storage devices such as thumb drives and small external hard drives. This passive data storage, called data at rest (DAR), enables us to conveniently transport and work with entire databases and other large amounts of information away from the normal security of an office or other controlled work place. However, with this mobile convenience and power comes increased risk of critical, sensitive data loss.

As laptops and data storage devices become smaller, they become easier to lose, through either neglect or theft. They fall prey to opportunistic thieves who want simply to sell the component. A worse scenario is that they fall into the hands of foreign agents or thieves who understand that the data is potentially far more valuable than the device it's on. If critical information is stolen, it could be held for ransom or used to compromise Army operations resulting in a failed mission or even loss of life.

People are easily distracted, forgetful and thieves can be very skilled and it is the responsibility of everyone -- soldier or contractor, officer or enlisted – to take the steps necessary to protect the sensitive information they carry with them.

Such steps include using available technology and procedures such as using approved encryption and passwording individual devices. When used together correctly, it is possible to deny data access to casual thieves. For sophisticated thieves with the knowledge and resources to compromise the protection, effective safeguarding will delay access until steps are taken to make the lost data useless or at least mitigate the potential danger.

Responsibility for DAR protection lies with local commands and individuals. Training is available and should be mandatory for anyone using MCDs. The Office of Information Assurance and Compliance website, <https://informationassurance.us.army.mil>, provides more details on DAR security. All MCD users should take the training and do what it takes to keep your mobile devices from becoming so mobile they leave your control. Make sure that through passwords, encryption and correct procedures that resting data is tucked in and protected from thieves that go bump in the night.