Commissioner's advice on how individuals can fully wipe their BlackBerry® and electronic devices (interview with BNN)

October 28, 2008

There are two basic measures to protect data on your BlackBerry device:

1) My number one recommendation is to use a password. This is like putting a lock on the front door. Using a password will prevent unauthorized access to your personal information. There are lots of options: complex passwords; time out periods (i.e. when you aren't using your device); and periodic challenges so that if someone else has your BlackBerry, it will lock-up after a set period of time. If someone were to enter the incorrect password too many times, all of the data would be erased.

2) For very sensitive data, users may want to consider the built-in content encryption. This feature works with the password to protect against physical attacks on the device and uses AES to encrypt the data stored on the device.

For enterprise customers, these safety measures can be centrally controlled by the IT Administrator using IT Policy.

For lost or stolen devices, enterprise customers can have the IT Administrator issue a remote "wipe" command that will remotely erase all of the contents. Consumers/individuals can get the same functionality from the BlackBerry® Unite! software (free download from RIM website).

Lastly, RIM has a published document for repurposing devices:

http://www.blackberry.com/btsc/search.do?cmd=displayKC&docType=kc&externalId=KB05099&sliceId=&dialogID=201270026&stateId=1%200%20201266506

There is a flow chart to follow depending on whether you are an individual user (BIS) or a corporate user (BES). A good practice in all cases would be to take a backup of your personal information with the Desktop Manager software and initiate the device wipe from the Options/Security screen before it leaves your control.