

▶ Thinking About Protecting Data on Portable Devices

Executive Insight Series
by Richard Mackey, Jr.

© Copyright 2007 SystemExperts Corporation. All rights reserved.

▶ Thinking About Protecting Data on Portable Devices

Protecting data on portable devices like USB drives, cell phones and Blackberries is critical in today's corporate environments. Strangely enough, though, at least some of the policies to deal the threats associated with such devices *should* already be in a company's repertoire.

The problem can be broken down into three classes of threat:

- ▶ Exposure of sensitive information or access when the device is sold or reused
- ▶ Exposure of sensitive information or access in the event of a lost device
- ▶ Exposure of sensitive information through inappropriate use

The first and second class of threat should be handled by media handling, data destruction and reuse policies. In other words, if the device is to be sold, recycled, or reused, it needs to be erased. This can be more easily said than done, however. While some cell phones provide a clear function, they may not erase the memory sufficiently to make the data irrecoverable by off-the-shelf software. Organizations should look closely at the effectiveness of built in features and employ other methods (e.g., overwriting all memory) in the event that the erase feature is simply deallocating the storage.

The second class, the theft problem, is more challenging. One approach is to establish a policy that sensitive data is not allowed on these devices. That can be problematic, especially in today's highly mobile executive community; many executives use their Blackberries for email more than their computer. Another approach is to use a commercial encryption product that encrypts the data as it is stored. This improves security, but makes the device more difficult to use. Not a great tradeoff, typically, in a device whose sole purpose is convenience.

It seems the only prudent approach is a combination of policy and technology, where critically sensitive email, messages, and documents are encrypted, and not readable on the handheld device (i.e., you'll have to wait until you get to your office or laptop). This is not a perfect solution by any

means, but the size of these devices lead them to be left on the seat of the cab, on the restaurant table, on in the plane more often that anyone would like to admit.

To protect against the third class, misuse, it is vitally important that organizations include restrictions on the use of these portable devices in their Acceptable/Appropriate Use policies.

While USB type devices should come under an organization's general Removable Media policy, unfortunately, they are regarded as a brand new problem and often slip under the radar. One policy that we have seen work is that there is a set of officially sanctioned devices that can be used by designated employees. There needs to be a corresponding process by which allowable devices are checked for viruses and other malicious code. The standard policies for removable media should apply to these devices including: encryption of confidential data, removal from company premises, and destruction.

Practical Measures to Take

- ▶ Set clear policies.
- ▶ Enforce policies through deployment of technology.
- ▶ Policies should address auditing, backup, encryption, and acceptable use.
- ▶ Allow only company-issued devices to be used.
- ▶ Implement a process by which allowable devices are checked for viruses and other malicious code.
- ▶ Limit USB flash drive usage to designated machines and staff. In particular, be sure to deploy technology to disable use of USB flash drives in highly sensitive environments.
- ▶ Encrypt contents to prevent unauthorized disclosure.
- ▶ Maintain records of data stored on removable devices.
- ▶ Centrally manage company-issued devices.