In the last column, security expert John Bumgarner and I looked at the potential for data leakage introduced through the use of small portable USB flash drives.

To counter the threats presented by USB Flash drives organizations need to act now. Organizations need to establish a policy which outlines acceptable use of these devices within their enterprises.

* Organizations should provide awareness training to their employees to point out the security risk posed by these USB Flash drives.

* The policy should require prior approval for the right to use such a device on the corporate network.

* Encrypting sensitive data on these highly portable drives should be mandatory because they are so easy to lose.

* The policy should also require that the devices contain a plaintext file with a contact name, address, phone number, e-mail address and acquisition number to aid an honest person in returning a found device to its owner. On the other hand, such identification on unencrypted drives will give a dishonest person information that increases the value of the lost information – a bit like labeling a key ring with one’s name and address.

* Physical security personnel should be trained to identify these devices when conducting security inspections of inbound and outbound equipment and briefcases.

Unfortunately, the last measure is doomed to failure in the face of any concerted effort to deceive the guards because the devices can easily be secreted in purses or pockets, kept on a string around the neck, or otherwise concealed in places where security guards are unlikely to look (unless security is so high that strip-searches are allowed). That doesn’t mean that the guards shouldn’t be trained, just that one should be clear on the limitations of the mechanisms that ordinary organizations are likely to be able to put into place.

Administrators for high security systems may have to disable USB ports altogether. However, if such ports are necessary for normal functioning (as is increasingly true), perhaps administrators will have to put physical protection on those ports to prevent unauthorized disconnection of connected devices and unauthorized connection of flash drives.

Because without appropriate security, these days your control over stored data may be gone in a flash.

* * *

John Bumgarner < mailto:john.bumgarner@cyberwatchinc.com > is President of Cyber Watch,
Inc. <http://www.cyberwatchinc.com>, a security consulting firm based in Charlotte, NC. John has a rich background in national security and international intelligence and security work.

* * *


MSIA: 18-month online Master of Science in Information Assurance offered by Norwich University; see <http://www3.norwich.edu/msia> for full details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2003 J. Bumgarner & M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.