

Seven Steps to Secure USB Drives

White Paper
July 2007

80-11-01600 Revision 1.0

SanDisk®

Even when used with the best intentions, the data stored on USB drives is generally not covered by routine company procedures such as backup, encryption, or asset management.

Introduction

Personal storage devices such as USB flash drives are more powerful than ever and have become ubiquitous in the enterprise environment. Originally designed for consumer use, these devices typically lack security, control and auxiliary management tools. Many employees don't think twice about taking work home, or out of the office, on the personal thumb drive they purchased at a local center for office supplies. With millions of people carrying around personal storage devices, these gadgets are being used both innocently to increase productivity and for other less legitimate purposes such as smuggling information out of the enterprise.

Big convenience, bigger challenge

Even when used with the best intentions, the data stored on USB drives is generally not covered by routine company procedures such as backup, encryption, or asset management. How can organizations keep track of the data entering or leaving the company via these devices? Keeping data secure has become a significant challenge for any IT department.

Recent Incidents

Recent events in the industry have been cause for concern, leading IT professionals to understand that new policies and technologies must be set in place to protect information being stored on personal storage devices. The following are just a few episodes that have driven the message home.

When a professor from the University of Kentucky discovered that his flash drive was stolen, private information for 6,500 former students was suddenly at risk. The data, including names, grades and Social Security numbers, left thousands of individuals exposed to the threat of identity theft, not to mention the violation of their privacy.

[Jon Swartz, "Small drives cause big problems," USA Today, 16 August 2006]

Flash drives with classified military information were up for sale at a bazaar outside Bagram, Afghanistan. The US Army realized that it had to secure USB drives, find a way to keep track of the devices, and ensure that the information could not be accessed by unauthorized personnel.

[Watson, P., "U.S. Military Secrets for Sale at Afghan Bazaar," Los Angeles Times (Latimes.com), 10 April 2006]

When an organization's information is stored on non-secure and personally owned devices, employees put their employer at risk every time they step out of the door.

Security Implications

When an organization's information is stored on non-secure and personally owned devices, employees put their employer at risk every time they step out of the door. Auditing companies are at risk of exposing account numbers, hospitals can be exposed if patient information falls into the wrong hands, and finance companies need to ensure that mission-critical data is not lost. Once company data falls into the wrong hands, the possibility of threats and risk is almost infinite. Organizations lose credibility, leave themselves open to lawsuits, and expose employees to ID theft or fraud – just to name a few of the concerns.

The risks from personal storage devices can be classified as follows:

- Data exposure due to device loss or theft
- Unauthorized data extraction
- Introduction of malicious code

Enterprise Concerns

With millions of USB storage devices in the marketplace, confidential company data is constantly on the move, and simultaneously at risk to loss or theft. The potential for damage caused by the loss of sensitive company data grows exponentially every day, underlining the need for proper security measures that cover these handy mobile storage devices. The following are some of the major security concerns related to their use:

Data leakage. To minimize the threat of data leakage, enterprises can start by limiting the use of USB drives to company-authorized devices.

Regulatory compliance. All organizations should ensure that they comply with applicable government and security regulations – such as SOX (Sarbanes-Oxley Act), HIPAA (Health Insurance Portability and Accountability Act), GLBA (Gramm-Leach-Bliley Act), California Senate Bill 1386, and FISMA (Federal Information Security Management Act) – to minimize the risk of data loss.

[Note: Not all enterprises are subject to all of these regulations] The first step is to set clear security policies and publicize them among employees. These policies can be enforced through use of technology that audits, tracks and backs up all information on mobile drives.

Lost data and support costs. Despite security measures, data may be lost or stolen, leaving the organization in a position to minimize the damage done. Issuing company-authorized USB devices enables the initiation of procedures to recover lost data and reduce the subsequent damage.

Possible Solutions

What can enterprises do to beef up security measures for personal storage devices? There are a number of hardware and software solutions ranging from data encryption to authentication, antivirus protection, and other monitoring options. Some solutions, such as blocked ports, encrypted storage devices and software encryption of data, do not address all that is required to ensure a comprehensive, secure solution for the majority of removable devices.

Seven steps to secure personal storage drives

Your organization can take the following steps to optimally secure personal storage drives, both on and off the network.

1. Always define and publicize your organization's policy for personal storage devices
2. Institute the use of company-issued personal storage devices
3. Make sure devices are fully encrypted
4. Make sure users cannot circumvent security measures
5. Maintain an audit trail of data stored on devices
6. Be able to recover data residing on personal storage devices
7. Make sure your enterprise solution comprehensively provides the ability to control the use of all removable devices, inside and outside the corporate environment, and to centrally manage company-issued USB drives

The value of portable storage devices in today's business environment is clear. Equally clear is the initiative organizations must take to integrate these devices with their storage and security policies. Today's enterprises can take steps to secure and monitor their data with technological solutions, develop robust policies to comply with regulations, and ensure the use of enterprise-ready personal storage devices.

For more information please visit www.sandisk.com/enterprise or e-mail enterprise@sandisk.com.

SanDisk®

SanDisk Corporate Headquarters
601 McCarthy Boulevard
Milpitas, California 95035-7932
Corporate Phone: (408) 801-1000
Corporate Fax: (408) 801-8657
www.sandisk.com

SanDisk® Corporation general policy does not recommend the use of its products in life support applications where in a failure or malfunction of the product may directly threaten life or injury. Per SanDisk Terms and Conditions of Sale, the user of SanDisk products in life support applications assumes all risk of such use and indemnifies SanDisk against all damages. See "Disclaimer of Liability."

This document is for information use only and is subject to change without prior notice. SanDisk Corporation assumes no responsibility for any errors that may appear in this document, nor for incidental or consequential damages resulting from the furnishing, performance or use of this material. No part of this document may be reproduced, transmitted, transcribed, stored in a retrievable manner or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written consent of an officer of SanDisk Corporation.

All parts of the SanDisk documentation are protected by copyright law and all rights are reserved.

SanDisk and the SanDisk logo are registered trademarks of SanDisk Corporation. Cruzer is a registered trademark of SanDisk Corporation, registered in the U.S. and other countries. Other brand names mentioned herein are for identification purposes only and may be trademark(s) of their respective holder(s).

© 2007 SanDisk Corporation. 80-11-01600 Revision 1.0, July 2007