

Put Security Policies in Place for Portable Storage Devices

Ruggero Contu, John Girard

Learn from the U.S. Department of Energy's troubles. If you deal with sensitive information, adopt strong security policies for portable storage devices.

NEWS ANALYSIS

Event

On 26 July 2004, U.S. Energy Secretary Spencer Abraham ordered Department of Energy (DOE) facilities around the country to stop all classified work on computers until security for removable storage devices is tightened. The order followed the loss of two computer disks containing nuclear weapons information at Los Alamos National Laboratory in New Mexico. It applies to Los Alamos and 16 other DOE facilities.

Analysis

Gartner has warned repeatedly that portable storage devices pose a serious security threat. These devices can be removed and used to leak sensitive corporate data, and can also be used to bypass security systems and introduce malicious software into a network. The U.S. Department of Energy announcement followed reports of a similar ban on portable storage devices by the British Ministry of Defence (ministry officials later announced that there was no outright ban, but rather a "flexible management approach in regards to iPods and similar devices that can move data from official systems").

Recommendations:

- Companies dealing with sensitive information should restrict the use of uncontrolled, privately owned devices with corporate PCs. The prohibition should include employees and external contractors with direct corporate network access.
- Security managers should adopt suitable policies for the use of portable storage devices, with advice on the main procedures to be followed for the eventual use of such devices. For example, policies should confirm the need for passwords and encryption of stored corporate data.
- Security managers should consider mobile data protection and firewall tools to help control the use of portable storage devices, to prevent the possible introduction of malicious code and minimize the risk of information leakage.

Analytical Sources: Ruggero Contu and John Girard, Gartner Research

Recommended Reading and Related Research

- "How to Tackle the Threat From Portable Storage Devices" — Businesses must ensure that procedures and technologies are adopted to securely manage the use of portable storage devices such as USB "keychain" drives. **By Ruggero Contu**
- "Magic Quadrant for Mobile Data Protection, 1H04" — In 2004, mobile data protection leadership requires centrally managed protection across a wide range of mobile platforms, including laptops, PDAs, two-way pagers and telephones. **By John Girard and Ray Wagner**

(You may need to sign in or be a Gartner client to access the documents referenced in this FirstTake.)

REGIONAL HEADQUARTERS

Corporate Headquarters

56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters

Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters

Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters

Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters

Gartner do Brazil
Av. das Nações Unidas, 12551
9º andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509