

NLAWARP White Paper Number 5

7 Steps to secure use of USB Sticks

USB “Sticks” – BIG CONVENIENCE - BIG CHALLENGE

Personal storage devices such as USB flash drives are more powerful than ever with huge capacities, stretching to Giga Bytes and have become ubiquitous in their use. Originally designed for consumer use, these devices typically lack security, control and management tools. Many employees don't think twice about taking work home or out of the office on the personal “pen drive”. These gadgets are being used both innocently to increase productivity and for other less legitimate purposes such as smuggling information out of companies.

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 companies keep track of the data coming in or leaving the company via these devices? Keeping company data secure has become a significant challenge for any IT department.

Many companies are only now beginning to set in place policies that will prevent unauthorised removable devices from entering the workplace. Their tiny size and ease of use means that any employee has the potential to download and store huge volumes of sensitive information about the company's operations. **Other devices such as iPods, Blackberries and mobile phone, can also now have Giga Byte storage capabilities. These can also plug into laptops and desktop PC's.**

It really happens

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

- ❑ A flash drive containing the personal information of 120,000 current and former patients of a Hospital was lost last year. The data included names addresses, social security numbers and identifying medical record numbers. The hospital has since banned the use of USB drives.

- A credit company hired a company to assess the security of its network, noting that the vulnerability of USB drives were of particular concern. The security company gathered all the worthless vendor giveaway thumb drives and planted a Trojan that, when run, would collect passwords, logins and machine-specific information from the user's computer, and then e-mail the findings back to the company. The drives were then scattered in the parking and smoking areas. Employees who found the drives plugged them into their computers the minute they got to their desks, initializing the flow of secure information outside the company.

7 STEPS TO SECURING PERSONAL STORAGE DRIVES

The following steps will help your company secure personal storage drives, both on and off the network.

1. Always define and publicise your company policy for personal storage devices.

Once you decide to take measures prohibiting the use of unauthorised USB devices, make sure you put these policies down in writing and create a plan to integrate them within corporate IT operations. Keep in mind that data can be copied to a wide range of mobile devices, including cameras, modems, network interfaces, printers, smart phones, and music players. Your policies should address the use of these devices in your organisation and work to deter data theft by making the information on stolen or lost drives inaccessible.

2. Institute company-issued personal storage devices. Although it is not practical to ban the use of personal storage devices, it is perfectly reasonable to limit their use to company-issued devices. Employees would not purchase a laptop at any electronics store and use it for working at the office, and should learn to follow the same standards for personal storage devices.

3. Make sure devices are fully encrypted. Because personal storage devices are easily lost or stolen, encryption is imperative. Furthermore, companies should ensure that 100% of the contents on the device are encrypted, so that data security is not left up to the device owner, but is handled automatically by the device.

4. Ensure that users cannot circumvent security measures. Most employees see USB drives as consumer devices similar to their cell phones or cameras, and don't see how critical password protection can be. Your company policies and USB devices should enforce security measures by making the use of passwords mandatory—and making sure the responsibility for protection is not left up to the employee.

5. Maintain an audit trail of data stored on devices. When administrators have complete control over which devices are used and how they are used, they can ensure the confidentiality and security of data. This is a must for both customer protection and legal requirements.

6. Have the ability to recover data that resides on personal storage devices. Make sure your total solution for USB drives can help you ensure business continuity through seamless device backup and the ability to restore or recreate lost or stolen drives.

7. Make sure your company solution is comprehensive enough to

- a. provide you with the ability to store information on secure USB drives
- b. control the use of all removable devices both inside and outside the corporate environment
- c. centrally manage company-issued USB drives.

encription limited are TIGER certified penetration testers, we already provide IT Security services to several Local Authorities and would welcome the opportunity to provide both references and a competitive quotation for your IT Security requirements.

**Encription Limited
Encription House
White Lodge
Bever
Worcester
WR3 7RQ**



NLAWARP PO Box 6733 Chingford, London E4 8UD Tel: 020 8524 2185
www.nlawarp.gov.uk Contact: mark.brett@socitm.gov.uk

© 2008 Copyright of this document is owned jointly by Socitm and encription

Non-Commercial and Public sector organisations may reproduce the contents of this document, so long as the source and copyright owners are acknowledged.