

» Risk Associated With USB Memory Sticks and High Capacity Storage Devices «

A white paper by Sam Wong, Siemens Insight Consulting



Advances in USB technology have introduced a number of convenient and physically very small devices that can store vast amounts of data. Removable USB storage media have become a very popular PC hardware technology. Users have found the small physical size, along with the large storage space, to be extremely convenient and easy to use. However, with this ease of use and universal connectivity of USB devices, there is now a growing risk to companies and their clients through the use and misuse of USB storage devices.

The biggest risk posed to companies is the theft of data by disgruntled employees or by recovering data from lost, stolen and misplaced USB storage devices.

"The use of unauthorised portable storage devices poses many dangers, not least for

the malicious code that they can introduce. High data capacity and transfer rates, and broad platform support mean that a Universal Serial Bus (USB) or FireWire (IEEE 1394) device has the capacity to quickly download much valuable corporate information, which can be easily leaked to the outside world." (Ruggero Contu, Gartner)

There are a number of methods and technologies that are available for companies to protect their data from unauthorised access. These methods are:

- Restricted usage or disabling of USB ports and devices
- Encryption of USB storage drives
- Restrict access to vital files and folders on critical servers
- Monitor access to critical servers by employees
- Limit the size of data transferable to USB storage devices
- Enforce acceptable usage policies for USB device usage

Other risks include viruses and USB media corruption. Viruses can be introduced onto company networks through USB devices.

Identity

Insight Consulting

www.siemens.co.uk/insight

SIEMENS

These can be mitigated through desktop firewalls and Intrusion Prevention Systems (IPS) and up-to-date anti-virus solutions. Media corruption can be mitigated through policy enforcement.

Restricted usage or disabling of USB ports and devices

Companies who are becoming aware of the threat of USB devices have begun to mitigate the risk by disabling the USB ports. There are a few logical methods available to disable USB ports. Two examples of which are listed below:

- Disable USB ports within the Bios and password protect the BIOS or disable the USB ports from within Active Directory Group Policy (<http://support.microsoft.com/?kbid=555324>). However, this is not suitable for USB input devices such as smart card readers, keyboards and mice
- Disable the addition of new hardware through the use of bespoke USB device management Active Directory management snap-ins (<http://www.windowsdevcenter.com/pub/a/windows/2005/11/15/disabling-usb-storage-with-group-policy.html>).

Disabling the USB ports takes a rather brute-force avoidance approach in mitigating the security risks associated with USB devices. The advantages of using USB devices are therefore negated by disabling USB ports.

Additional USB management solutions allow for the controlled mitigation of risk through technology. The solution allows for a detailed addition of specific USB devices to be used. Devices can include printers, storage devices etc.

Encryption of USB storage drives and data

There are a number of products on the market available that can provide additional security to USB devices and to systems that have USB ports available. A number of these offer USB media encryption with additional 1,2 or 3 factor authentication. The multiple factor authentication is normally a combination of some of the following:

- USB device — Obtaining physical access to the USB device and the data stored
- Biometric Authentication — User identification based on individual human characteristics such as fingerprints, voiceprints or retina scans
- PIN or password — Personal Identification Number (PIN) remembered by the USB device owner
- Encryption certificate — Certificate to identify the user, the certificate is commonly held on a smartcard and then authenticated against a certificate authority server.

USB device security products

Following reports from various security analysts including the Ministry of Defence and Gartner, a number of companies have produced products to mitigate the security risks from USB devices. These products attempt to reduce potential attack vectors arising from USB and firewire storage devices.

USB devices with encryption

A number of companies are now producing USB storage devices with a built-in encryption feature. These USB devices have both a public (plainly visible) and a private (encrypted) storage area. These devices are deemed to be personal to the user and are unencrypted using fingerprint authentication. These products protect against the exposure of important data to third parties. Encryption can be secured using passwords or biometrics.

USB devices with read/write access

Some USB devices are now produced with a read-only switch, much like floppy disks. When these USB devices are connected to users' home computers, the read-only setting should be enabled so that viruses and malware cannot spread to the device and then subsequently introduced to a corporate network. These products should also be used in conjunction with a desktop anti-virus solution.

USB device restriction software

Software solutions can integrate with the active directory domain and restrict certain devices on company desktops. The software can be configured against not only USB, but FireWire (IEEE 1394), parallel, IrDA and other types of communication ports. The software has a repository of the acceptable devices that are allowed to connect to the desktop machine. All other devices not on the list are blocked by default and logging of the event is registered, if required.

USB device encryption software

Other than hardware based encryption products, companies have also marketed software based products to encrypt storage media data. This software integrates with corporate directories such as Novell's eDirectory and Microsoft's Active Directory and can be set-up to use certificates to encrypt data held on USB devices.

Data file transfer restriction software

As part of the protection of vital client data, software installed onto the server can protect vital files by limiting the size of files that can be transferred to a USB device. The file size limits within the software should be configured to be less than the size of the smallest critical files, such as database backups and important client information. Using this software as an isolated solution would not be ideal as files may be spanned across a number of smaller zip files and transferred over a period of time.

A number of product links with these features are listed below:

- Beyond If Solutions have a number of USB security devices. Their products incorporate biometrics for encryption and physical access
- The Clipdrive Biometric USB drive from Optimal Access uses biometric authentication to encrypt sensitive data
- StorageCrypt 2 encrypts data located on internal hard drives as well as portable hard drives and USB

- GFI's EndPoint Security controls USB device activity; providing full auditing and device control
- Aladdin's USB Port Protector restricts the types of USB devices connected to the end points of the company infrastructure. However, this product does not provide encryption or restrictions on size of files transferred to the USB devices
- Safend offer a number of products to enhance USB security. Safend do not offer a complete all in one solution, each product performs an individual function. However, Safend do offer USB port protection, USB data encryption and auditing of USB device activity
- CDLock by Smartline restricts the types of removable media to be used on a desktop PC. Restrictions can be based on the the types of devices utilising a USB device "white list" of acceptable devices and also based on the time of day. Permissions can be set via the Active Directory Group Policy and also granted on a temporary basis
- SecureWave's Sanctuary Device Control software offers a number of features in a one product solution. Port protection focuses on a number of communication ports including USB, FireWire (IEEE 1394) and IrDA. Policies and restrictions can be set through the Active Directory Group Policy. The software also offers auditing of device activity and, importantly, data encryption on sensitive data.

USB device security control software

There are several products available that may offer a number of features to enhance USB device security. The features of some of the products are listed below. Product selection should be based on individual requirements.

The technical features to enhance USB device security are as follows:

- Devices are restricted by user, user group and machine specific access control lists
- Configurable device "white list" to prevent installation of unknown devices
- Full protection to disconnected and remote computers
- Customizable event notification when access is denied
- Auditing and reporting functionality
- Device restriction on a variety of communication ports and devices
- Silent installation and deployment using MSI technology
- Easy encryption mechanism without the necessity of installing additional software
- Ability to integrate biometric authentication.

Restrict access to vital files and folders on critical servers

Files or systems vital to the company should be deemed restricted and should be limited to those who require regular and/or frequent access. Access to critical files and folders should be granted and removed in accordance with the role and as soon as possible to maintain access controls.

Access to files and folders can be monitored and automatically restricted through the use of the following systems:

- IDS – File access should be monitored by file access logging or by installing host based intrusion detection systems on the relevant servers. It is vital that the IDS policies are tuned to ignore unimportant information and that adequate notification is sent to system administration teams as and when necessary. Custom alerts may be set up to alert on the unauthorised copying of data files from the server.
- Identity Management - Access to files and folders within an Active Directory environment can also be controlled within the Group Policy for users or computers. Insight Consulting recommends either an IDM solution or through changes to the Active Directory Group Security Policy. It is very important to note that any monitoring and logging system requires additional resource to examine the log files and investigate alerts. There will be no advantage gained in deploying an IDS system and enabling high level logging on critical systems if the log files and monitoring systems are not periodically checked for alerts and anomalous activity.

Limit the size of data transferable to USB storage devices

As part of a technical solution for mitigating the risks of USB devices, some software products are capable of limiting the size of files copied to a USB device. This solution is totally configurable. Products such as Sanctuary Device Control by SecureWave provide this functionality. The ideal configuration would be to set the maximum allowable transfer size to be less than the size of the smallest critical file.

Enforce acceptable usage policies for USB device usage

As part of any other security mechanism installed into a company's IT infrastructure; policies should be put in place so that employees are fully aware of acceptable usage. There should be a separate section within the IT security and acceptable usage policy on data retention on laptops and other mobile devices. The important aspects of the acceptable computer usage policy of note are:

- USB devices should only be used for transfer and not for storage
- Data on mobile devices should be transferred to data servers at regular intervals
- Data should not be transferred from servers to USB media if unauthorised to do so

Risk Associated With USB Memory Sticks and High Capacity Storage Devices

- Policies should also warn against misuse and attempts of unauthorised access. Part of the policy should also warn of any disciplinary or legal proceedings to follow
- Any policies should also be in compliance with BS 7799, the RIPA act and the Data Protection Act
- Personal USB devices should not be used on company hardware (if applicable).

U3 Technology

Advances in USB technology and weaknesses in the Windows operating systems can allow malicious malware located on USB devices to compromise a Windows based operating system. The presence of the Windows Autorun feature and weaknesses in the Direct Memory Access (DMA) allow for malicious files to be executed. Bruce Schneier has released a cryptogram detailing the vulnerability and how to protect against this attack vector (http://www.schneier.com/blog/archives/2006/06/hacking_compute.html). The recommendations are to disable the autorun feature and to restrict certain types of USB devices. Insight Consulting offers technical advice and solutions that reduce risk from these attack vectors.

Threats from malware

In addition to the risks of exposure through the acquisition of company data, there are also threats to company infrastructure of viruses and malware transferred from employees' personal home computers. Insight Consulting can help in the implementation of distributed computer security including anti-virus agents and host based intrusion detection / prevention systems for the desktop.

Business justification

As with any enhancement to the IT security infrastructure, a cost benefit analysis should be performed in conjunction with the client so that risks and benefits may be fully understood. The ultimate aim for any consultant visiting a client should be on this premise: How much is the data worth in terms of reputation and financial cost against the cost of deploying a number of new security technologies.

References

<http://www.usbflashdrive.org/>
<http://blogs.ittoolbox.com/security/adventures/archives/portable-storage-device-security-8995?rss=1>
http://insight.zdnet.co.uk/0_39020415_39159600_0.htm
http://www.schneier.com/blog/archives/2006/06/hacking_compute.html
<http://www.biometrics.org/>
<http://www.beyondifsolutions.com/>
http://www.marketwire.com/mw/release_html_b1?release_id=128638
http://www.optimalaccess.com/cart/shop.php?s=product_info.php&products_id=36
<http://www.magic2003.net/>
<http://www.gfi.com/endpointsecurity/?adclickid=7302976>
<http://www.aladdin.com/partners/findresults.asp?id=183>
<http://www.safend.com/63-en/Safend.aspx>
<http://itmanagement.earthweb.com/security/article.php/3530476>
<http://www.beyondifsolutions.com/>
http://www.marketwire.com/mw/release_html_b1?release_id=128638
http://www.optimalaccess.com/cart/shop.php?s=product_info.php&products_id=36
<http://www.magic2003.net/>
<http://www.gfi.com/endpointsecurity/?adclickid=7302976>
<http://www.aladdin.com/partners/findresults.asp?id=183>
<http://www.safend.com/63-en/Safend.aspx>
<http://itmanagement.earthweb.com/security/article.php/3530476>



Key Benefits

- Reduced risk of data theft
- Reduced risk of data loss and/or corruption
- Enhanced controls of access to company critical data
- Implementation of security across the network infrastructure
- Employee understanding of USB device usage policies

Insight Consulting is the specialist Security, Compliance, Continuity and Identity Management unit of Siemens Communications and offers a complete, end-to-end portfolio encompassing:

- Security
- Continuity
- Managed Services
- Compliance
- Identity Management
- Training

Siemens Insight Consulting subscribes to the CISO Listed Advisor Scheme (CLAS) and CHECK services. We're also certified against BS7799 and are a preferred supplier of services to the UK Government and are an accredited Catalyst supplier.

If you'd like to find out more about how we can help you manage risk in your organisation, visit our web site at www.siemens.co.uk/insight
Siemens Insight Consulting
Tel: +44 (0)1932 241000
Fax: +44 (0)1932 236868

www.siemens.co.uk/insight