

» Securing USB Memory Devices to Reduce Risks to IT Infrastructure «

Mitigate security risks from USB storage devices through encryption, anti-virus agents, usage policies and Active Directory controls



Advances in USB technology have introduced a number of convenient and physically very small devices that can store vast amounts of data.

The mobility, ease of use and certified conformity of the USB standard has resulted in the widespread usage of USB devices for both the office and home. The interconnectivity, ease of use and the ability to store vast quantities of data expose companies to a number of risks.

A company may be exposed to theft of data through the use of high volume storage devices either by disgruntled employees or through stolen or misplaced devices. It is now possible to store many gigabytes worth of data on USB devices such as the iPod and removable hard drives.

The storage of company critical data on mobile storage devices also exposes companies to potential data loss through media corruption and misplacement.

Companies' and client confidentiality may be exposed by unauthorised access to removable storage devices by third parties. Further damage may then be caused by loss of reputation and competitors gaining advantages through the acquired data.

Memory devices also provide new scope for virus attack vectors. Viruses and malware may spread to personal removable devices, which, if then used in company environments, may then spread onto an infrastructure evading gateway anti-virus systems. The new U3 smart technologies can automatically access applications without user interaction, increasing risks when sharing USB devices.

Companies are becoming aware of this risk and some have completely disabled USB ports to the extent of filling the ports with expandable foam to forbid USB device usage. However, this also restricts the advantages of using USB devices, taking the approach of avoidance rather than control.

Identity

www.siemens.co.uk/insight

Insight Consulting

SIEMENS

Securing USB Memory Devices to Reduce Risks to IT Infrastructure

USB drives are now large enough to store entire operating systems that can be booted from laptops and PCs to bypass user and smart card technology. If misplaced laptops are obtained by third parties, unsecured data can be easily retrieved by people who have knowledge of basic Windows and PC architecture.

PCs should be configured so that operating systems installed on USB devices cannot be accessed.

The latest generation of USB storage devices are beginning to integrate security measures to mitigate the risk of data loss or data theft. Some devices use fingerprints or passwords as a means of restricting access through authentication.

Other security measures also limit access to read-only so that viruses cannot be transferred from home systems on to company networks and infrastructure.

How Siemens Insight can help

Siemens Insight Consulting can review current security infrastructure, procedures and policies to understand and mitigate current levels of risk.

There are a number of countermeasures that can help to reduce the risk of using USB storage devices, these include:

- The introduction of encryption technology to protect data and confidentiality against misplaced or stolen USB devices and laptops
- The deployment of intrusion detection systems (IDS) on critical servers, files and folders to monitor and protect against unauthorised access by disgruntled and restricted employees
- The introduction of identity access management to completely remove access by employees who have left the company
- Advice on Active Directory security to restrict the addition of unrecognised hardware devices
- A review of anti-virus architecture and policies to reduce exposure to virus attack vectors
- Reviews of acceptable usage policies and guidance on policies regarding USB storage devices and acceptable

computer usage. Policy changes may enforce the non-storage of company data on removable storage devices or banning the usage of iPods and other USB storage devices in the workplace.

Siemens Insight Consulting may integrate any technical solution with any existing architecture within a company; technologies such as smart cards and identity management solutions.

The types of usable USB devices can be restricted through technological solutions; restrictions can be based on the type of device (e.g. USB printers and authorised USB storage devices) or the size of data transferred to the storage device.

Data held on mobile computing devices should be encrypted using industry standards to restrict exposure of company data to third party employees, although users should be advised not to store data on USB devices and USB devices should only be used to transfer information between laptops and PCs to mitigate risk against data loss.

Technical solutions may extend to restricting the types of USB devices and connectivity ports so that personal hardware cannot be used in conjunction with company equipment.

Servers critical to company business continuity should have limited access so that limited numbers of employees may access vital files and folders.

Anti-virus and intrusion detection system infrastructure should be applied across the company infrastructure including laptops and desktop PCs to limit exposure by malicious software.

Benefits

By taking a multi-pronged approach, a number of risks are reduced. The main benefits are:

- A reduced risk of data theft through storage device acquisition
- Secure means of data transfer using USB devices
- Enhanced control over acceptable devices used within company infrastructure



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

- Employees have a full understanding of acceptable usage of USB devices
- System administrators know which servers are critical and who has attempted to access them
- Desktop systems are fully protected from malicious attacks and viruses
- Competitors do not gain an advantage through stolen data or damaged reputations.

Conclusions

Insight can provide consultancy on mitigating risks to companies through the usage of USB devices and peripherals. Insight can provide a number of potential solutions as a multi-pronged approach.

Customers

Insight Consulting has performed security audits for a number of various clients including British Telecom, HBOS Plc and Lloyds TSB Plc.

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

Siemens Insight Consulting subscribes to the CERG 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