



**Technical Note: 03/2006**

## **Peripheral Access Management**

Issued 08 May 2006

### **Abstract**

This document provides guidance to organisations on managing the security risks of peripheral access devices, such as USB data keys and personal music players.

### **Disclaimer**

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by NISCC. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

NISCC shall also accept no responsibility for any errors or omissions contained within this document. In particular, NISCC shall not be liable for any loss or damage whatsoever, arising from the use of information contained in this document or its references.

**National Infrastructure  
Security Co-Ordination Centre**  
PO Box 832  
London  
SW1P 1BG

Tel: 0870 487 0748  
Fax: 0870 487 0749  
Email: [enquiries@niscc.gov.uk](mailto:enquiries@niscc.gov.uk)  
Web: [www.niscc.gov.uk](http://www.niscc.gov.uk)

## KEY POINTS

- This document is a guide as to how organisations should manage the security risks of peripheral access devices.
- The size of peripheral access devices is decreasing whilst their capacity to store large quantities of information is increasing. Peripheral access devices can therefore be used to remove very large quantities of information from organisations' IT systems.
- Some peripheral devices such as portable music players can also be used as data storage devices to inject or extract information and malicious software to or from computer systems.
- Some types of peripheral device can be used to bypass computer operating system access controls and security at the hardware and software level.
- Peripheral access devices should be controlled using a mixture of policy, people, process and technical controls as appropriate to the assessed level of threat and business impact-of-compromise to the organisation.
- The deployment of peripheral access management solutions can be difficult for large, complex organisations and may require changes in previously accepted working practices.

## STRATEGIC BUSINESS CONTEXT

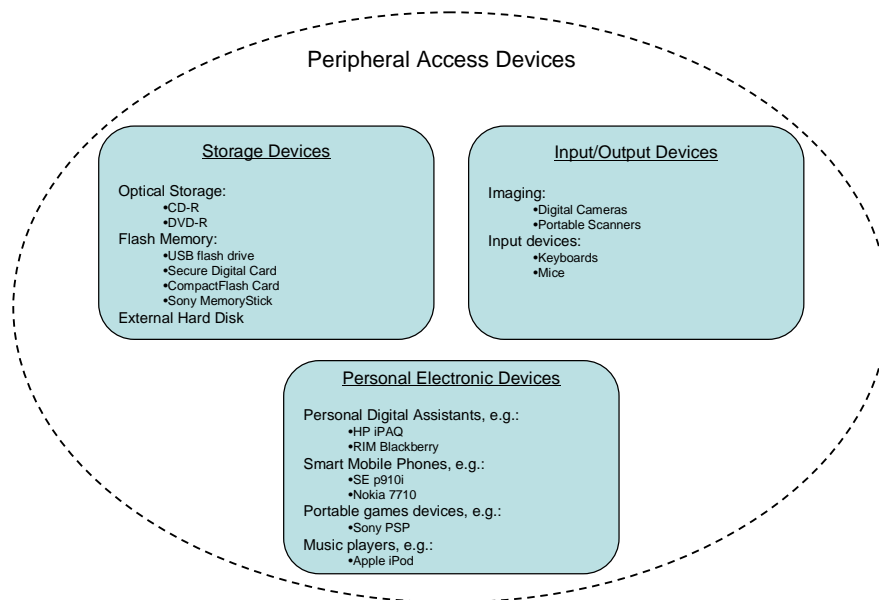
### Overview

1. Peripheral access management covers the processes and technologies intended to control the use of devices such as USB flash drives and external hard disks connected to computers such as PCs, laptops and servers. Peripheral devices are typically used to expand the functionality of a system by providing additional storage or input / output channels.
2. The control of peripheral devices has been a security issue for several years as floppy disk drives and tape streamers have been in use for some time. However, in recent years, the security context has changed:
  - peripherals have decreased in cost allowing consumers to purchase more sophisticated devices;
  - peripherals used for data storage have increased enormously in capacity;
  - many peripherals have decreased in physical size; and
  - the technologies used for connecting peripheral devices have dramatically increased in data transfer speed and functionality.
3. Small, high capacity devices with sophisticated functionality have become commonplace. USB flash drives, hard disk personal music players, Personal Digital Assistants (PDAs) and other devices are often used in an organisation's offices by members of staff.

4. The capacity and performance offered by floppy disks and CD-ROMs is no longer sufficient for the demands of modern organisations. The demand for portability of information has driven an increase in the capability and proliferation of peripheral device technology.
5. This paper is intended to raise awareness of the security risks associated with peripheral devices and to present a number of options to help organisations to manage the risks.

## Scope

6. The diagram below summarises the divisions of peripheral device that are addressed in this paper.



**Figure 1: Types of peripheral access devices**

7. The boundaries between devices are blurred as personal electronic devices offer both storage and input/output functionality. For example, USB flash drives are available that provide both wireless connectivity and storage capability. Storage devices can also be considered to be an input/output channel as they can readily be moved between systems to transfer data.
8. Most devices within scope are commonly available and are relatively inexpensive. The storage capacity of peripheral devices is significant from a security perspective. The following is a sample of current maximum capacities:
  - USB flash drive (also known as USB stick or pen drive): 4GB;
  - Secure Digital (also known as SD card and found in cameras, PDAs and mobile phones): 2GB;
  - external hard disks (within music players): 80GB; and
  - external hard disks (standalone): 1000GB (1TB) and higher.

## Technical background

9. A wide variety of peripheral devices exist; however, they are largely dependent on a small group of connectivity technologies as described below.

### **Wired**

#### *Universal Serial Bus (USB)*

10. USB is a widespread serial bus technology. The design was standardised by the USB Implementers Forum, with devices being compliant with v1.0, v1.1 or v2.0 of the specification. The current implementation, v2.0 Hi-speed, delivers transmission speeds of 480 Mbps (for comparison Fast Ethernet is 100 Mbps).
11. USB supports multiple classes of device, which are enumerated when a device is connected. The specification defines the following classes: hub (controller for devices), human interface (such as keyboards), printer, imaging and mass storage (such as flash drives).

#### *FireWire*

12. FireWire is a high speed serial bus, also known as iLink and IEEE 1394. The standard was designed by Apple Computer Inc and standardised by the Institute of Electrical and Electronics Engineers (IEEE). The current implementation, FireWire 800 delivers transmission speeds of 800 Mbps.
13. FireWire is commonly used for the connection of audio/visual devices and external hard disks.

#### *PC Card*

14. PC Card is also known as PCMCIA and CardBus. PC Card is essentially an external PCI (Peripheral Component Interconnect) expansion bus and commonly used to extend laptop computer functionality. PC Cards deliver transmission speeds of approximately 500 Mbps and are commonly used to connect networking devices.

### **Wireless**

#### *Bluetooth*

15. Bluetooth is a radio communications standard developed by Ericsson and standardised by the Bluetooth Special Interest Group. Major standards include v1.0, v1.1, v1.2 and v2.0. The current version delivers transmission speeds of 2.1 Mbps. Range varies but is usually less than 10 metres. Bluetooth is commonly used to connect mobile phones and to allow point to point network communication.

#### *Infrared*

16. Also known as IrDA, this is a set of protocols using infrared for communications, developed by the Infrared Data Association. Several protocols exist; the latest version, Very Fast Infrared, delivers speeds of 16 Mbps. Range is limited to less than one metre. IrDA is commonly used for mobile phone connectivity and point to point network communication.

#### *Wireless USB*

17. Wireless USB (WUSB) is a new radio technology which has yet to be standardised. Speed varies but should deliver 480 Mbps at a three metre range and 110 Mbps at 10 metres<sup>1</sup>.

### *Other Wireless Technologies*

18. The risks of wireless technologies, such as 802.11a/b/g, have been explored in other research and are not discussed in this paper. However, controls outlined in this paper for restricting use of peripheral access devices may also be appropriate to control use of wireless connection devices.

### **Overview of security concerns**

19. With the potential exception of Wireless USB, none of these protocols are designed to be secure and have limited authentication and encryption functionality.
20. FireWire and USB are of particular relevance due to the following features:
  - very high data transfer speeds;
  - built into most desktop and server class computer systems; and
  - a number of inexpensive peripheral devices connect using these standards.

### **Information held on devices**

21. On devices with smaller storage capacities, such as mobile phones, the information held tends to be limited to contact lists, SMS messages and emails. On larger capacity devices, such as portable hard disks, information can be anything up to a mirror of a workstation hard disk or a backup of significant portion of a network drive.
22. The information held on larger peripheral devices may be nearly anything stored on a network. This has significant implications for large repositories of sensitive data such as file shares and databases.

### **Current control and management environment**

23. Peripheral device control and management has been a feature of the security landscape for many years. Peripherals such as floppy disk drives have been available for decades and therefore some controls are likely to exist. Often, existing controls consist of:
  - security advice against theft or loss of devices;
  - reporting processes following theft or loss, largely to arrange device replacement;
  - anti-virus protection on workstations; and
  - a limited extension of laptop mobile computing security policies, often without associated technical controls such as authentication and encryption.

## **RISKS**

### **Generic technical vulnerabilities**

#### **Lack of encryption**

24. Most peripheral devices do not provide data encryption functionality by default. Encryption of data in transmission is also very unusual, as most peripherals are designed to be connected locally. This means that plain text data may be read directly from a device or potentially intercepted while in transmission.

### **Lack of authentication**

25. Authentication controls on devices themselves are uncommon. Mobile phones and Personal Digital Assistants (PDAs) offer basic authentication by means of SIM codes or passwords. These forms of authentication rarely protect the data stored on flash memory within these devices, as the flash memory can often be physically removed from the device. This means that data may be readily accessible once physical access to the device has been obtained.

### **Size and portability**

26. Many Personal Electronic Devices and peripheral storage devices are designed to be highly portable. Certain types of flash memory such as MicroSD (also known as TransFlash) are designed to be as small as possible. MicroSD cards are around 15x11x1 mm in size (smaller than a five pence coin) and have a capacity of 1GB<sup>2</sup>.
27. External hard disks are bulkier than flash memory, although 1.8" drives will fit in a jacket pocket. Larger capacity disks will fit inside a small bag or briefcase. A 1TB external hard disk drive is 44x270x173 mm in size, weighing 2.5 kg<sup>3</sup>.
28. This means that considerable amounts of data can be held in a small device that is easily concealed. Devices can also be hidden in plain sight because the devices are so common, particularly USB flash drives, mobile phones and PDAs. Physical control of small peripheral devices is therefore extremely difficult. A visual inspection will not reveal whether an individual is carrying these devices.

### **Speed**

29. Several types of connectivity, particularly USB 2.0 Hi-Speed and FireWire, offer extremely fast data transmission speeds. It is therefore feasible to copy large amounts of data in a very short space of time.

## **Vulnerabilities specific to USB storage devices**

### **Windows Autorun**

30. Microsoft Windows Autorun allows the automatic execution of a program from a peripheral device. The file `autorun.inf` must be present on the device, which specifies the file to be run.
31. Autorun is restricted to CD-ROM and fixed disk drives. Autorun on USB mass storage devices, particularly USB flash drives, is intended not to work. However, external CD-ROM drives that use USB for connectivity<sup>4</sup> will successfully Autorun. The vulnerability is that Autorun could be used to automatically execute malicious software on a system the moment the device is connected.
32. In addition, USB flash drives are being marketed with the explicit feature of supporting Autorun<sup>5</sup>. This works by using UDRW technology, where a portion of the flash drive is presented as a CD-ROM to allow Autorun to operate. UDRW devices also provide a hidden memory zone which is not directly accessible to users<sup>6</sup>. It is possible that malicious software could be held within the UDRW or hidden memory zones.

### **Bootable USB devices**

33. It is possible to boot from USB storage devices on a system where the BIOS supports this functionality<sup>7</sup>. Assuming the system supports USB booting, the process to create a USB boot device is straightforward and involves copying the appropriate boot files to the device. USB boot devices can be built to boot into the Windows or Linux operating systems.
34. Once booted via a USB device, an attacker may have full privileged access to the system including the fixed hard disks and potentially data stored on them, if encryption is not in use. An attacker would also be able to use diagnostic tools to analyse the system in detail, as might occur during computer forensics, and copy data off the system onto another removable device. For example, encrypted information could be copied for cryptanalysis at the attacker's leisure.

### **Vulnerabilities specific to FireWire devices**

35. Direct Memory Access (DMA) is an essential function of modern systems where devices are able to access memory without the request going via the CPU, to improve performance. FireWire uses DMA to access system memory without the intervention of the operating system. It has been demonstrated that an Apple iPod (a portable music player with an internal hard disk) is able to arbitrarily read or write memory on certain versions of the Apple MacOS, FreeBSD and Linux operating systems<sup>8</sup>.
36. The demonstration noted that it was not possible to cause the effect on Windows XP operating systems due to the different system architecture. However, a successful exploit of Windows operating systems using this technique should be considered a possibility in the future and would allow an attacker to access fundamental data structures in system memory, and thereby bypass security.

### **Threat Profile**

#### **Unauthorised copying of data**

37. Peripheral storage devices may be used to copy significant amounts of sensitive data, presenting a threat to confidentiality if the data is accessed by an unauthorised individual. This threat may manifest from members of staff that have some level of authorised access to systems.
38. The threat of unauthorised data copying has existed since portable media have been available. Now that the storage capacity of devices has increased the potential impact of the threat has increased as such significant amounts of data may be copied.
39. Furthermore, the small size of many peripheral storage devices means that the devices may be straightforward to remove from a site. Large portions of network file stores or entire databases may be copied and removed from an organisation's premises by a member of staff or an attacker with physical access.

#### **Loss of device**

40. The loss of a peripheral device is a threat that has been recognised by many organisations, particularly those with mobile staff equipped with laptop

computers. The potential scenarios are the unintentional loss of a device or intentional theft by an attacker. These situations present a threat to confidentiality if sensitive information is obtained and passed to an unauthorised party. A threat to availability may exist if information is unique or the device is critical to the organisation

41. Thousands of electronic devices are lost each year meaning that the occurrence of unintentional loss may be the most frequently occurring threat. Lost property may be returned, disposed of, or sold.
42. Security researchers have purchased second hand storage devices and determined that often large quantities of data remain recoverable<sup>9</sup>, illustrating the potential threat to confidentiality.

#### **Unauthorised access to peripheral**

43. The threat of unauthorised access to a device may be the result of a theft. However, an attacker may not need to physically remove the device to access information as the data may be copied while the device is in place.
44. An attacker may make a copy of information, presenting a threat to confidentiality or they may alter information on the device, presenting a threat to integrity.

#### **Malicious software vector**

45. Malicious software (malware) can be defined as software designed to infiltrate or damage a computer system without the consent of the user. Examples include viruses, worms and Trojan horses. Traditionally, malware was spread by the physical exchange of floppy disks. As the use of floppy disks has decreased, 'network aware' malware began to use alternative vectors such as e-mail and network services.
46. Peripheral storage devices may be used in a similar fashion to floppy disks, presenting malware with a vector for infection. The exchange of malware via physical channels therefore remains a current threat. The threat may be more serious due to increased storage capacity, meaning that larger and more sophisticated malware could be transferred.
47. There is a risk that a "peripheral storage aware" program may be able to spread via storage devices by detecting when it is connected to a system. A malware author could theoretically 'inject' a number of infected devices into an organisation with the intention of causing damage.
48. There is also a risk that undocumented or potentially malicious features may be incorporated by manufacturers of peripheral access devices.

#### **Inadvertent use of wireless technologies**

49. A number of peripherals use built in wireless functionality, which may be inadvertently deployed by an organisation that restricts wireless technology. This may occur where wireless keyboards, mice or presentation tools are deployed.
50. The organisation may be exposed to the inherent insecurities of wireless technology, such as passive traffic monitoring, while not appreciating the security implications that exist. This may result in threats to confidentiality or integrity of data as it is transmitted.

### **Targeted information harvesting**

51. One key threat of storage devices is the malicious use of hidden storage within a peripheral device. Hidden storage may be achieved by the device containing an area of memory that is not visible to the user by default. Alternatively, hidden storage may be achieved by physically concealing additional storage within a peripheral device, eg, via use of a second memory chip. The hidden storage can hold malware with a defined objective, such as obtaining all files with a particular filename. An attacker could plant or inject the compromised device into an organisation, allow it to harvest information and then retrieve it. Alternatively a Trojan horse program could be conveyed via one route, which is designed to detect and then copy targeted information onto a peripheral device which the user then removes from the system and connects to a less secure Internet connected system.
52. Devices explicitly designed to capture data, such as inline hardware keyloggers are available for consumer purchase<sup>10</sup>. They are straightforward to use; require no software installation; and are able to record several million keystrokes. A keyboard with a built-in keylogger is also available, which records the keystrokes typed into it<sup>11</sup>.
53. In early 2005, a major theft from the Sumitomo Mitsui Bank in the City of London was attempted using information gathered from inline hardware keylogger devices<sup>12</sup>. The attempt was prevented by law enforcement officers that learned of the attempt before it was completed.

## **IMPACT TO UK CRITICAL NATIONAL INFRASTRUCTURE**

54. The significance of peripheral device security is not to be underestimated. The preceding sections have described the devices and their associated risks. Peripheral devices add an attack vector and, due to their ubiquity, substantially increase the attack surface of an organisation.

### **Exposure**

55. A review of an organisation may reveal a large number of deployed peripheral devices. Some devices will be owned and supported by the organisation while others will be the personal property of staff and contractors.
56. CNI organisations may be exposed to the threats posed by peripheral devices. The degree to which a specific organisation is exposed will depend on a number of factors, including:
  - number of staff;
  - number of technically capable staff;
  - types of data held electronically;
  - sensitivity of data held electronically;
  - dependence on electronic information systems;
  - level of authorised usage of peripheral devices;

- level of unauthorised usage of peripheral devices; and
- effectiveness of existing controls.

57. A review of peripheral device use will help to reveal the degree of exposure to peripheral device threats.

## Impact

58. The impact of a security breach that may arise from one of the risks described will depend on the nature of the organisation and the extent to which it is exposed to the risks.

59. The impact of a breach may be very significant as the risks associated with peripheral devices are wide reaching. One of the key issues with peripheral access devices is that they can bypass the robust technical measures organisations may implement to achieve perimeter security. Organisations can thus be exposed to threats that they had otherwise thought were appropriately mitigated by centrally controlled technical measures, such as firewalls, anti-virus, etc.

60. The results of a security breach may include the scenarios summarised below:

Impact type	Description
Inadvertent or unauthorised disclosure of information (including espionage)	This may occur through attacks designed to exfiltrate information, e.g. Trojan horses, or other malicious software that may be installed on peripheral access devices.
Unauthorised alteration or modification of information (including fraud)	This may occur through attacks designed to alter information, e.g. Trojan horses, or other malicious software that may be installed on peripheral access devices.
Disruption to the availability of information (including deliberate sabotage)	This may occur through disruptive attacks that are deliberately designed to damage the organisation concerned, e.g. use of Trojan horses or other malicious software hidden on peripheral access devices.

## PERIPHERAL ACCESS MANAGEMENT

61. The tables below set out a series of suggested controls that can be used to manage the risks related to peripheral devices. Controls should be selected and modified according to a risk assessment. A risk assessment will provide a detailed understanding of the current level of exposure and the potential impact at a specific organisation.
62. A blanket ban on peripheral devices is not likely to be practical due to the amount of necessary peripherals such as keyboards and mobile phones. The tables below provide baseline control options and also enhanced control options which are likely to be applicable for organisations subject to higher levels of threat and/or impact of compromise. In this table, certain controls relate explicitly to devices privately owned by staff while others relate to devices issued and owned by the organisation.

### Policy controls

63. This table provides a set of example policy statements relating to the control of peripheral devices.

Control	Baseline	Enhanced
<b>Approval</b>	Personally owned devices may be permitted for use following explicit approval from the information security team.	Personal storage devices are not permitted.  Other peripheral devices may be permitted following explicit approval from the security team.
<b>Usage</b>	Peripheral devices should be used in accordance with relevant security policy controls for mobile computing, such as password use and theft prevention.	As for baseline.

Control	Baseline	Enhanced
<b>Usage in secure areas</b>	Personal electronic devices and storage peripheral devices are not permitted in secure areas such as communication or server rooms.	<p>Personal electronic devices and storage peripheral devices are not permitted in areas where sensitive information is processed or handled.</p> <p>At sites where sensitive information is regularly handled, peripheral devices are not permitted on site unless owned by the organisation and strictly accounted for and controlled.</p>
<b>Connectivity to organisation owned equipment</b>	Explicit approval from the information security team should be sought before personal electronic devices are connected to the organisation's computing equipment.	Personal electronic devices should not be connected to the organisation's computing equipment.
<b>Management and support</b>	<p>Peripheral devices should be managed, supported and controlled by the relevant technical teams.</p> <p>Personal electronic devices are the responsibility of the owner.</p>	Peripheral devices should be managed, supported and controlled by the relevant technical teams.
<b>Device access control</b>	Peripheral storage devices should use security measures to prevent unauthorised access such as power on or login passwords, file encryption, etc.	Peripheral storage devices should use approved security measures to prevent unauthorised access.

Control	Baseline	Enhanced
<b>Device connectivity control</b>	<p>Technical controls to prevent security breaches from peripheral devices should be in place on workstation systems.</p> <p>Explicit approval from the information security team should be sought before using any form of wireless connectivity.</p>	<p>A centralised technical control system to prevent security breaches from peripheral devices should be in place on systems with connectors for peripheral access devices.</p> <p>Wireless devices of any sort should not be used.</p>

### People controls

64. This table provides a set of suggested controls relevant to staff behaviour and activity.

Control	Baseline	Enhanced
<b>Management awareness</b>	Senior management should be made aware of the risks associated with the use of peripheral devices. Senior management should be involved in sponsoring peripheral access management controls.	As for baseline, including executive management.
<b>Staff awareness</b>	Staff should be made aware of the risks of using peripheral devices.	<p>Staff should be made aware of the risks of using peripheral devices.</p> <p>Awareness programmes should consist of direct security training of staff.</p>
<b>Roles</b>	Peripheral access management and associated controls should be the responsibility of a member of the information security team.	Peripheral access management and associated controls should be the responsibility of a senior member of the information security team.

Control	Baseline	Enhanced
<b>Physical search</b>	None.	Where security guards are permitted to search staff and visitors entering or leaving secure areas, search procedures should include peripheral access devices. However the small size of such devices means that this control should not be relied upon to detect all peripheral devices.

### Process controls

65. This table provides a set of suggested controls relevant to ongoing process to manage peripheral devices.

Control	Baseline	Enhanced
<b>Documentation</b>	Peripheral access management policy statements should be part of a security policy, code of conduct or staff handbook. Evidence should exist of staff agreement to the security documentation.	As for baseline.
<b>Device approval</b>	A process should exist for approving devices owned by the organisation and by staff. The process should involve a technical analysis of the peripheral and a risk based decision.	A inventory of approved peripheral devices should exist. Peripherals should be subject to a rigorous accreditation process.  The process should include a technical analysis of the peripheral and an investigation into the manufacturer and supply chain of the device. A risk based decision should be made by the information security team to determine whether the device is included on the approved list.
<b>Loss reporting and</b>	A process should exist to enable staff to	A process should exist to enable staff to report the

Control	Baseline	Enhanced
<b>investigation</b>	report the theft or loss of a peripheral device. The information security team should make a risk decision as to whether an investigation should be carried out.	theft or loss of a peripheral device. Instances of loss should be investigated by the appropriate team.  The investigation should include an analysis of the sensitivity of the data held on the device, the likelihood of exposure and possible mitigation steps.
<b>Peripheral technology monitoring</b>	A process should exist to monitor the current threats and vulnerabilities related to peripheral devices.	A process should exist to monitor the current threats and vulnerabilities related to peripheral devices.  A report of this process should be produced on a regular basis that compares the results to the usage of peripherals within the organisation. The report should also include recommended mitigation actions.
<b>Audit and review</b>	A process should exist to review the use of peripheral devices on a regular basis. The review should include a sample of users and associated devices.  The results of the review should examine compliance with policy statements and technical controls. The results should identify risks and recommendations and be submitted to the information security team.	As for baseline, with larger review sample size and a summary report submitted to senior management, explaining the business risk.

## Technical controls

66. This table provides a set of technical controls for technical peripheral access management.

Control	Baseline	Enhanced
<b>Lockdown BIOS</b>	None.	<p>On high risk systems:</p> <ul style="list-style-type: none"> <li>• Disable system BIOS peripheral functionality on high risk systems; and</li> <li>• Disable system BIOS USB boot functionality.</li> </ul>
<b>Lockdown Autorun functionality</b>	Ensure workstations are locked when left unattended as Autorun will not work when systems are logged off or locked.	<p>On high risk Microsoft Windows systems:</p> <ul style="list-style-type: none"> <li>• Disable Autorun functionality by setting the registry setting:</li> </ul> <pre>HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun</pre> <p>to the value: FF</p>
<b>Lockdown physical connectivity</b>	None.	On very high risk systems physically remove or disable unused peripheral sockets.

Control	Baseline	Enhanced
<b>Malware protection</b>	Ensure that a real time virus scanner is running on systems.	<p>On high risk systems:</p> <ul style="list-style-type: none"> <li>• Scan peripheral devices for malware using an isolated secure virus scanner system (often known as a 'sheep dip') before connecting to systems.</li> <li>• Block import of executable content using approved software.</li> </ul>
<b>Secure the data held on peripheral devices</b>	<p>Where peripheral storage devices are required to hold sensitive materials ensure that data is encrypted and that authentication is required:</p> <ul style="list-style-type: none"> <li>• deploy file encryption software;</li> <li>• deploy hardware devices with built-in authentication and encryption functionality, such as USB flash drives with built-in biometric controls.</li> </ul>	Only storage devices with built-in or centrally managed encryption and authentication can be used.
<b>Centralise control for peripheral devices access</b>	Use Windows Group Policy to disable peripheral device functionality <sup>13</sup> . Note that this is only possible on the Windows Server 2003 version of Active Directory and later.	Deploy a centralised Peripheral Access Management tool that controls the connection of devices and allows audits of existing device usage to be performed.

## Peripheral access management software

67. A number of products are available to help centrally manage the risks associated with peripheral devices. The table below summarises the control functions that may be offered by products. A product may offer multiple control functions.

Peripheral access management functionality	Description
Data encryption	Products that provide encryption for files and directories where the decision to encrypt is made by a centralised policy and enforced by software installed on systems.
Device encryption	Products that provide encryption for peripheral storage devices where the decision to encrypt is made by a centralised policy and enforced by software installed on systems.
Peripheral device audit	Products that provide the functionality to centrally monitor and review the peripheral devices that are currently deployed within an organisation.
Peripheral device connectivity control	Products that provide the functionality to control connectivity or access to devices based on a centralised policy and enforced by software installed on systems.

## Peripheral access management deployment

68. The majority of the controls described in the previous section will be difficult to apply over a large and complex IT estate, particularly the deployment of a centralised management system.
69. A business decision should be taken as to how resources should be deployed, for example, whether to make individual system changes or to use centralised management tools. Regardless of the approach adopted, the deployment of controls may be a large and costly project.

### Project considerations

70. Several factors should be considered when approaching centralised peripheral access management. These include:
  - the project should be sponsored by appropriately senior management from the earliest stages to help ensure that the project receives the support and resources that are required;
  - the scale of a deployment will require a commensurate budget; and
  - a business case should be developed that includes:
    - the risks of peripheral devices;
    - the controls provided by the deployment;
    - any potential post deployment cost savings, such as reduced support calls due to smaller amounts of unauthorised software and hardware being installed on standard build systems; and
    - a comparison with alternative options, showing differences in cost and risk management effectiveness.
71. An increasing number of products are commercially available to provide peripheral access management. Products should be carefully tested before selection to help ensure the product will meet the organisation's security and management needs. Testing should be sufficiently rigorous to determine faults and shortcomings in less mature products.
72. Where possible, peripheral access management products should be integrated into existing security management tools. This will reduce the administrative overhead from the introduction of a peripheral access management product.
73. The product should be used in coordination with security processes that manage the use of peripheral devices. For example, it may be appropriate to have a peripheral device access request process.

### **Culture change considerations**

74. Organisations that have deployed peripheral access management systems have noted that key challenges are the technical deployment and the required change in staff culture.
75. The restriction of peripheral devices may cause a significant change in working practices for many staff. Extensive effort will be required in raising awareness of the risks associated with peripheral devices and obtaining commitment from members of staff. Significant working culture changes should be driven by the senior staff and should include every staff member that uses IT equipment.

## Glossary of Acronyms

GB	Gigabytes
IrDA	Infrared Data Association
Mbps	Megabits per second
PDA	Personal Digital Assistant
SMS	Short Message Service
TB	Terabytes
USB	Universal Serial Bus
WUSB	Wireless Universal Serial Bus

## References and further reading

- <sup>1</sup> [http://www.usb.org/developers/wusb/About\\_WUSB2.pdf](http://www.usb.org/developers/wusb/About_WUSB2.pdf)
- <sup>2</sup> <http://www.sandisk.com/Products/Default.aspx?CatID=1099>
- <sup>3</sup> <http://www.lacie.com/products/product.htm?pid=10128>
- <sup>4</sup> [http://www.targus.com/us/product\\_details.asp?sku=PACD010U](http://www.targus.com/us/product_details.asp?sku=PACD010U)
- <sup>5</sup> [http://www.hsc-us.com/consumer/usb\\_flashdrive/UDRW.html](http://www.hsc-us.com/consumer/usb_flashdrive/UDRW.html)
- <sup>6</sup> <http://www.udrw.com/en/tech/index.php>
- <sup>7</sup> [http://www.usb.org/developers/devclass\\_docs/usb\\_msc\\_boot\\_1.0.pdf](http://www.usb.org/developers/devclass_docs/usb_msc_boot_1.0.pdf)
- <sup>8</sup> <http://md.hudora.de/presentations/firewire/2005-firewire-cansecwest.pdf>
- <sup>9</sup> <http://news.bbc.co.uk/1/hi/technology/4229550.stm>
- <sup>10</sup> <http://www.keyghost.com/USB-Keylogger.htm>
- <sup>11</sup> <http://www.keyghost.com/securekb.htm>
- <sup>12</sup> [http://www.theregister.co.uk/2005/04/13/sumitomu\\_bank/](http://www.theregister.co.uk/2005/04/13/sumitomu_bank/)
- <sup>13</sup> <http://support.microsoft.com/default.aspx?scid=kb:en-us:555324>