

# NETWORK DEVICE AUDIT



## QUICKLY IDENTIFY WHAT DEVICES ARE USED ON YOUR NETWORK

One of the most commonly asked questions by IT management staff is if USB attached type devices are prevalent within a network?

Our surveys suggest that they are, and they have slipped largely unnoticed into common usage without any consideration to control or security.

### BUSINESS RISK IMPLICATIONS:

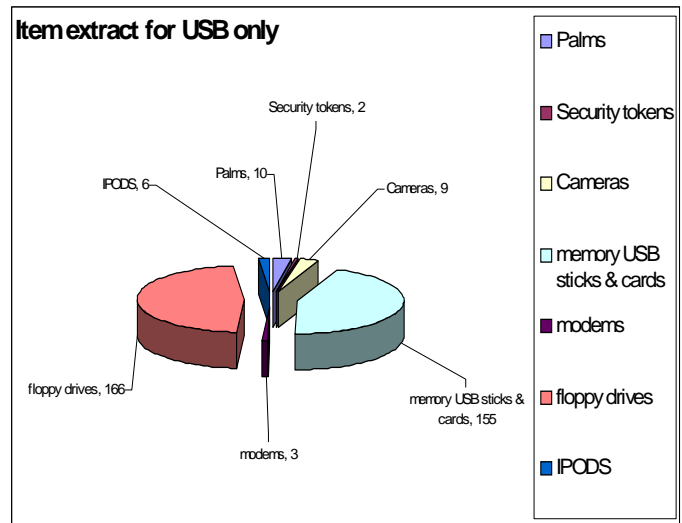
As a consequence the following issues have emerged:

- Virus and Spyware carried into the network on mobile devices, rendering gateway controls useless.
- Hardware Keyboard loggers easily inserted to covertly intercept passwords and login credentials.
- Loss of confidential information due to the sheer abundance and simplicity of attached memory devices.
- Erosion of the standard desktop configuration from attached device misuse and the associated support burden.
- A route for the installation of unauthorised applications (Software licensing and copyright infringements).

### EXAMPLE DEVICES

- Blue tooth devices
- External disk drives (CD, DVD, CDR, DVDR etc.)
- Ipods and similar media players
- USB memory sticks
- Flash cards
- Digital Cameras
- Smart phones

### MEASURING THE PROBLEM:



Our device audit consists of a collector being installed on a single PC that is connected to the rest of the network.

The scan typically takes a 1-3 hours and the information is compiled centrally with negligible effect on either network traffic or of the host machine being audited. No software is installed on any of the machine being audited.

The audit will only operate on windows machines and requires an administrator account or equivalent to run. The scan operates via remotely analysing the local registry of each PC. The registry having information about all devices plugged into that machine from the time the last OS was installed.

*Note it's also possible to audit internal drives, local printers, wifi usage etc, but the more information requested, the longer the scan takes.*

## Reporting and Scope:

Audit all devices and accessories that are connected to the workstation and identifying possible policy breaches and security issues.

Analyse if devices such as USB memory keys, I-pods and other portable media devices have the potential to transport harmful malicious code into the network or to act as a medium to remove confidential data from the company.

Wifi and Bluetooth are communication protocols that if not controlled allow unauthorised access to the network, bandwidth abuse and uninhibited content exchange; as such identifying their usage across all workstation is one of the first stages to managing the risk.

Accessories that now ship as standard such as DVD, CD'R drives allow unrestricted data copying and understanding who has the ability to write/author CD and DVD volumes is useful as it quantifies the issues beyond attached memory devices.

ITEM	Number	%
Palms	10	1.4
Security tokens	2	0.3
Cameras	9	1.3
memory USB sticks & cards	155	21.8
modems	3	0.4
floppy drives	166	23.3
IPODS	6	0.8

- Identify all device usage across all workstations (*on the basis they are accessible on the network*).
- Identify hardware keyboard loggers (Spyware tools).
- Identify communication asset items (IDE, USB, Root, SCSI, PCMCIA).
- Understand what devices constitute a threat.
- Understand the type and scope of accessories used within the network.
- Benefit from know exactly what needs to be managed.
- Full itemised report by workstation and device along with management style executive summaries.

## Example Report:

Device Name	Device Class	Bus	Model ID	Detection Date	Host(s)
256MB USB2.0FlashDrive USB Device	Disk drives	USBSTOR	USBSTOR\Disk256MB__USB2.0FlashDrive2.00	02/08/2006 21:46	ROBERTK
3SYSTEM USB FLASH DISK USB Device	Disk drives	USBSTOR	USBSTOR\Disk3SYSTEM_USB_FLASH_DISK_1.00	02/08/2006 21:46	ROBERTK
B4F SLIM USB Device	Disk drives	USBSTOR	USBSTOR\DiskB4F__SLIM_____2.00	02/08/2006 21:46	ROBERTK
ChipsBnk Flash Disk USB Device	Disk drives	USBSTOR	USBSTOR\DiskChipsBnkFlash_Disk_____2.00	02/08/2006 21:46	ROBERTK
Conexant D480 MDC V.92 Modem	Modems	PCI	PCI\VEN_8086&DEV_24C6&SUBSYS_542214F1&REV_01	02/08/2006 21:46	ROBERTK
CRUCIAL USB DRIVE USB Device	Disk drives	USBSTOR	USBSTOR\DiskCRUCIAL_USB_DRIVE_____1.12	02/08/2006 21:46	ROBERTK
Dell TrueMobile Bluetooth Module	Bluetooth Devices	USB	USB\VID_413C&PID_8000&REV_1266	02/08/2006 21:46	ROBERTK
disgo disgo USB Device	Disk drives	USBSTOR	USBSTOR\Diskdisgo__disgo_____4.31	02/08/2006 21:46	ROBERTK
disgo USB Device	Disk drives	USBSTOR	USBSTOR\Disk____disgo_____4.31	02/08/2006 21:46	ROBERTK
Easy Disk USB Device	Disk drives	USBSTOR	USBSTOR\DiskEasy__Disk_____2.00	02/08/2006 21:46	ROBERTK
ECP Printer Port (LPT1)	Ports (COM & LPT)	ACPI	ACPI\PNP0401	02/08/2006 21:46	ROBERTK

### OTHER SECURITY AUDIT SERVICES:

- **Vulnerability Scan:** Detecting network & host exploitable conditions.
- **Security policy and procedure review:** Contrasting industry best practices.
- **Wifi and IM detection:** Discovery of unauthorised transport comms.