What Do You Mean … 'Where Is It!'

Its Here Somewhere…

With business PC costs around $800+ and coupled with software, install charges etc. this rises to $3,000+. So an organisation with 1000 PC's has around $3.0M invested as a bare minimum for their desktops, plus other support, devices, network, lines, resource and infrastructure.
And don't even think about the security aspects on top of that!

If you viewed your IT assets as a vehicle fleet, would you want to know where your vehicles are and who is using them? Is the cost going to be so dis-similar?

Hardware audits are the basis for gaining and maintaining control of your assets. One assumes every organisation would want to know where their assets are going and if they're 'leaking' at all.

I thought we should have a bit of discussion and look at audit considerations in in a few articles.

A few of the benefits of auditing you IT asset pool includes:

- Validates what assets you really have
- Is essential for corporate asset governance
- Identifies models, types, state and condition
- Is required for Software Audit proof
- Assists strategy, support and planning elements
- Clearly identifies the location of assets
- Required for financial accounting
- Validates a logical (network) audit
- Clarifies warranty requirements and costs
- Deters theft

Begin With The End In Mind

Rather than 'sea gulling' an audit (run around, flapping, and making noise…) a better approach may be to consider the following:

- **What data** –Have a purpose for the collection and don't waste time collecting unnecessary data. Remember, an audit is a snapshot in time, it should be concise and accurate.
- **How** – An electronic audit is the fastest method and should provide in-depth information (software etc.). And a physical audit confirms and identifies non network devices. You may need to consider a hybrid approach or carry out both. More on this latter
- **The Output** – Make sure you have the ability to collate and manipulate the data to extract and report on the information you require.
- **Support elements** - You can gain allies and potential financial support by asking other departments what data they may require too. The IT architects, security and support people should be interested. The finance people would also benefit and potentially business areas will require the information too.

- **Location, Location** – Identify where the devices may be located as access to, timing (disruption) and defining count accuracy is necessary. Do not forget non-network attached devices, backup devices (in cupboards!) and devices used off premise i.e. at home. Support personnel can generally assist with this.

Audit Methods

The two methods of conducting a hardware audit are:

- Physical – Also seen as 'manual' although in today's world we can use electronic data gathering methods, so maybe semi-automated sounds better.
    - Pros
        - Very accurate count of physical devices.
        - Great method for verifying an electronic tools accuracy.
        - Physical contact allows verification of asset tags (or the application of asset tags).
        - Can be sped up with RFID technology.
        - Contact with campus admin/management allows interaction and communication.
        - Ability to audit all devices in an area regardless of network status and location.
        - Use of smart phone technologies and scanners can lower cost and increase speed.
    - Cons
        - Slow to extract internal attributes and software.
        - Is time & resource intensive.
        - Virtual devices require investigation via consoles.
        - Auditor costs, scan devices and tags need to be allowed for.
        - Collation of data into some a reportable form can take time.
- Electronic – This is a preferred method for most, but is no silver bullet
    - Pros
        - Data is gathered as part of BAU so minimal additional time is required
        - Is repeatable (daily) with minimal additional time required
        - Reporting should be fast (tool dependent)
        - Gathers in-depth device attributes including software.
        - Most basic audits can be achieved without a client install in modern tools
    - Cons
        - Requires a tool, to be in place, tested for accuracy and which suits the technology base. (Several may be required).
        - Generally has high implementation cost plus ongoing training and support.
        - Accuracy is dependent on the application collection mechanism e.g. access etc.
        - Only works for network enabled devices.
        - Network security may restrict access to device.
        - May not pick up attached devices such as screens/printers etc.
        - Definitely won't pick up devices secured off the network
        - Requires an extremely well run network for location data to be accurate.

There is a definite case for both forms of auditing either simultaneously and separately depending on the circumstances. Electronic auditing is great for the ongoing snapshots with the manual audit providing periodic verification. While there has been an attempt to remove the need for manual audits (generally by well-meaning software companies …) the reality is manual audits are still required.

In the next article, we'll look at the specifics to consider in a manual audit.

Contact us at www.bursol.co.nz for support of your audits.