



Take control of Your Network Costs

The IT resources of your business - back-end infrastructure, standard operating environment, printers and other peripherals - are what allow employees to be productive. Unfortunately, if adequate controls are not in place, the potential for abuse of these resources is high.

Some transgressions such as printing a personal document on a company printer have a negligible impact, but other activities such as file sharing, downloading music and using non-business applications can have a substantial impact on infrastructure and productivity.

Employees' activities have the potential to expose and damage internal systems (e.g. running un-authorised programs), generally unwittingly. Restricting what employees can do, however, could be considered excessive, so the key is to find the balance between practical limitations and user autonomy.

The first step is to design and implement a SOE.

What is a SOE?

A SOE, or "Standard Operating Environment" is essentially a PC management methodology which reduces the cost of maintaining the PC's and increases their reliability and availability to the end users. The philosophy behind a SOE is to standardise as many aspects of the PC fleet as possible so that a minimum number of configurations need to be supported, administered and upgraded.

Benefits of a SOE:

To be effective, standardisation should be introduced and enforced (using features of the operating system) in the PC hardware, the operating system, and the application set used by an organisation.

The benefits of a well-designed and implemented SOE include:

- Reduced support costs
- Increased PC availability
- Increased manageability



Change Control

Implementing a standard system is useless if there is no mechanism to keep it standard. An enforceable (see *lockdown*) change control process which documents and tracks all significant changes to the environment is essential to realise the ongoing cost savings and productivity gains of an SOE.

Lockdown

The term 'lockdown' refers to using security features and policies available in the operating system to restrict the user's ability to re-configure their PC. This is required to ensure that PC's implemented in a 'standard' manner remain standard.

The SOE is the principal productivity tool for your employees, and when dealing with operating systems it is often necessary to protect employees from themselves. Users like to customise their systems, and in many cases this results in problems and crashes and frustration all round.

The number one enemy of a standard operating environment is the well meaning staff member who knows about PC's and "fixes", adjusts or installs applications themselves. Such changes - even if technically sound - introduce variances into individual PC's that complicate their management; often nullifying benefits of an SOE.

The degree of lockdown varies from site to site, but typically users are prevented from installing new applications, running un-authorized applications (e.g. games, ICQ, Messenger), editing the registry, installing or re-configuring drivers and in some cases even modifying the desktop.

Effortless PC Rebuild

If a PC can be re-installed with a minimum of effort, troubleshooting software corruption problems becomes trivial. A PC whose configuration for whatever reason becomes troublesome can typically be rebuilt in the vicinity of 30 - 40 minutes, simply by booting from a 'build' floppy disk, have an administrator answer a small number of prompted questions, and waiting for the automated build process to complete. Once this process is complete, the user can continue with their work on a 'clean' installation.



Application Management

Users' application settings and data are stored centrally in the directory on a fileserver so they can be accessed from any workstation.

In this way, users' shortcuts, applications, settings and data will follow them no matter which PC they login to. This provides a useful contingency feature allowing any user to use a spare or vacant PC should theirs develop a hardware fault or for some reason require a rebuild.

The philosophy behind this approach is that workstations are treated as a "terminal" to access data that is stored centrally on a file server. Any hardware fault at a workstation will result in relatively minor disruption, as there will be no data loss (as the user's data is stored on a server) hence another workstation can be located for the user to logon to the network and resume their work. File servers on the other hand, have backup schemes in place to ensure that no data loss occurs in the event of any hardware issue occurring at the server.

Permissions are granted or revoked by the administrator simply by adding users accounts to groups. There is no requirement for the administrator to visit the user's PC. An added advantage with this mechanism is that software licence auditing is made trivial - a count of the members in a centralised application group determines the number of licences required.

Desktop Management Tools

Desktop Management Tools can be implemented as part of a SOE deployment. While not an essential element of a SOE deployment, there are useful Open Source (i.e. free) tools that can be implemented securely that don't add to software licensing costs. These tools allow an administrator to remotely assist users to troubleshoot and resolve issues, and perform other activities that are usually performed by physically visiting the PC.

Back-end (Server) Controls

The next step in controlling network costs is to ensure that appropriate back-end controls are in place.

Employees should only have access to the server resources they need - file systems, back-up folders, mail servers and so on. When controls are too loose, the potential for employees stumbling across sensitive information or damaging important files increases dramatically. Assuming that the system has been configured properly, users should not need access to information about the company's internet proxy servers, firewall, server relationships and so on.

As with desktop management, access to file server resources is controlled through the management of permission's. Permission's are granted or revoked by the administrator simply by adding users accounts to groups. There is no requirement for the administrator to visit the user's PC.

Resource Management

Another area which should not be overlooked is Resource management. Most businesses make use of CD/DVD burners, colour printers, scanners and so on - but they are easily used for non-business purposes as well, and managers need to be diligent in preventing excessive personal use.

Computer media such as blank CDs and photo paper are handled like ordinary stationery, which can result in large hidden costs if their distribution is not managed effectively.

One way of doing this is to place these resources in the hands of designated staff that can process all requests as part of their everyday function and thus monitor usage.

Printers should be networked, which allows their access to be controlled, user quotas and reporting can be put in place to monitor usage.



Implementation

As a guide, an initial SOE image will take 2 – 3 days to develop. This image will then be used by a designated user (or small group of users) to test and evaluate before the SOE is deployed throughout the organisation.

Once the SOE image has been tested and approved, PC's can be typically rebuilt in less than 1 hour. However during the initial implementation, a migration step may be required, to move important user data from their local workstation to the server before the workstation PC can be rebuilt.

Once your requirements and environment are understood we can provide a quotation before commencing.

Zero Effort Networking (ZEN) is experienced in accurately identifying computer network problems and acting swiftly to fix them. Since 1996 we have helped clients implement stable, reliable computer networks that take the worry out of network management. For further information you are welcome to contact us.

Zero Effort Networking Pty Ltd
ABN: 38 082 434 446
Telephone: 02 9676 3541
Facsimile: 02 8569 2012
Email: info@zeroeffortnetworking.com.au
Web: www.zeroeffortnetworking.com.au
Office: Suite 15, 18 Third Avenue, Blacktown NSW 2148

No part of this publication may be reproduced without written permission of the authors. Copying and distribution by any means is strictly forbidden. Additional copies may be obtained for free by contacting Zero Effort Networking.