



---

Best Practices for  
Increasing  
Security and  
Reducing Cost

---

**White Paper**

## Best Practices in Desktop Security

In the current climate (post NIMDA and CodeRED) desktop security is a very serious priority for any organization. But just being concerned about the effect of malicious virus's will not make your organization secure from hostile intent. Here are some of the best practices that iTCO Solutions Inc. has seen:

- Educate your users about security. One of the easiest ways to obtain passwords is to randomly call employees, say you are from IT doing something urgent and you need their password to do it. Regularly send emails to your employees reminding them of your corporate policy to never reveal passwords by any mechanism. Smart users are your first line of defense.
- Use better passwords. First enforce strong passwords, 8 characters or more, with no dictionary or name words. Then rotate this password monthly and do not allow duplication. Then do a spot audit of all your administrators, they are often the weak link with the highest access. They will often override the system and prevent themselves from having to change their password. Check local desktop passwords as well as network passwords.
- Secure and encrypt personal data. Ensure that the file system that the user writes their data to does an authentication check (i.e. check who it is accessing data), allowing just administrators and the user full access. For a device that is not physically secure (laptops etc.), you should consider encrypting the part of the disk which is used to store documents. The theft of information is potentially a much greater threat than the denial of service attacks typical of viruses.
- Antivirus with push update. Yes, just having anti-virus software, even with scheduled update of signature files, is not enough. Smart organizations ensure that the signature files can be centrally pushed and re-scanned on demand. This allows the organization to heal from an attack very quickly.
- Install Service Packs. Do not delay installing service packs and patches unnecessarily. As soon as an O/S vendor has posted a patch on its web site, the truly malicious hackers are the first to read it and exploit it. Install the patches before the hackers can deploy their attacks. Ask your administrators what their policy is for deploying security patches is? Check they specify a minimum time that is deploy to the whole organization.
- Develop a secure desktop culture. Organizations that are successful with security foster an appropriate culture with their desktop devices. Users should not expect complete freedom with their workstation. Ask your administrators about the steps involved in installing an O/S? If it sounds similar to the steps you took to install your last O/S at home and involves a lot of "click next", then your organization maybe seriously be at risk. The effort to secure a corporate desktop is much higher than a home system, fully featured means fully at risk.

- Personal Firewall. Traditionally desktop devices are isolated from the unpredictable world of the internet by network firewalls. A good strategy with firewalls is to make them like onion skin with multiple walls that hackers have to break through. If you are relying on a limited number of firewalls, or one monolithic firewall for protection, then personal firewalls are very cost effective.

## Best Practices: Reducing the Desktop Cost

Desktop cost can spiral out of control without some positive intervention from IT groups. Here are some of the most beneficial ways that organizations have reduced cost at the desktop:

- Reduce running applications at the desktop. The more applications you run and support at the desktop the more expensive your costs will be. Reduce applications from the desktop with 2 initiatives. First, eliminate duplicate functionality by standardization (see next). Second, for applications that deploy frequent updates or have a high mortality rate (application dies on the desktop), move them to execute exclusively on servers. Server based computing is good for in house developed applications that change regularly and do not get the QA time on diverse desktop configurations.
- Standardization. Diversity is the agent of chaos and cost at the desktop. IT organizations should standardize on the smallest number of supported hardware platforms, operating systems and core applications. Best in class organization will support one or two operating systems, one office productivity suite, and one email package. These standards are the basis for developing a deployable unit that includes the standard O/S and core applications.
- Don't fix – replace. Don't tie up a user's time trying to fix a complex issue at their desk. Have spares on hand pre-configured and just replace it. If your standards project was successful this will be a breeze. If the users data is safely stored on a SAN (Storage Area Network) then this will be even easier. Don't even try to fix the issue back at the lab; just re-image the box back to standard, if the issue was not hardware related the unit can join the "spares" inventory.
- Remote control. Don't let your help-desk and administrators walk to desktops, or spend hours trying to visualize the issue. Use a remote control agent that allows help desk personnel and administrators see and fix issues over the network.

- Culture. Too much freedom at the desktop can be very pleasant for the user community, but the ensuing chaos is very expensive for an organization. The users do not often equate their freedom with the reliability of their desktop, nor do they ever recognize the cost of that freedom. IT organizations have a tough time finding the right balance between a locked down desktop and totally open O/S. Here is a test you can apply to yourself as a user; Can I Install Applications, Play Games, Change My Network Settings? If you answered yes to any of these questions then you are either an Administrator, or you work in a highly profitable organization that can afford this degree of user autonomy.
- Proactive desktop development. Successful desktop organizations tend to spend as much, if not more of their budget, on efforts to develop desktop solutions than field administrators to fix issues. In other words, they spend more on proactive desktop solutions, than reactive solutions. Unsuccessful desktop organizations tend to be heavily reactive, and as a whole much more expensive. Fixing an issue through development before it gets to the thousands of desktops at your organizations has a high ROI.

*Simplify IT*  
**iTCO**  
*your eBusiness Partner*  
[www.itcosolutions.com](http://www.itcosolutions.com)

---

iTCO Solutions Corporation  
P.O. Box 610090  
Redwood City, CA 94061  
United States

<http://www.itcosolutions.com/>

Enterprise Sales Team Contact  
Ryan Edwards  
National Accounts Manger  
Tel: 650-367-0514  
E-Mail: [redwards@itcosolutions.com](mailto:redwards@itcosolutions.com)