Global Information Assurance Certification Paper

Highly Available PC's
First Step in
Business Continuity for Executives

Joseph Fraher

GSEC Security Essentials Certification

Practical Assignment
Version 1.4b
Option 1
Date Submitted
December 20, 2003

Abstract

There are many ways to make users adhere to rules that are in their best interest. Local Policies and Domain policies are great for enforcing such rules. Forcing users to save data to a network drive is easily achievable through such policies. Enforcing these policies is another issue. Very often Network and Systems Administrators are faced with the problem where directors, managers, executive personal and the like, do not want such policies applied to them. These executive users often have enough influence in the organization to make them exempt from these policies, preventing you as the Administrator from protecting the users that need the protection the most. These executive users are often more comfortable with their data on their local hard drive and are unwilling to save their data to the network where it can be backed up regularly. They fail to realize that if the hard drive on their PC fails, all their data is often lost or at the very least, costly to recover. It will be your responsibility to recover this data and you will surely have an uncomfortable situation to deal with. By telling this executive "I told you to save your data to the network" certainly is not going to speed your ascend up the corporate ladder and may cost you your job. So how do you, as an Administrator of this network, protect these executive users from themselves and ensure that these systems stay highly available?

This paper will address the availability portion of the CIA triangle as it applies to Windows XP Professional. This paper will also suggest how to make these systems highly available through the use of hardware and software, avoiding the conundrum associated with enforcing company policy on those who are exempt from it.

Introduction

The first step in making sure a system is highly available is to identify the points of possible failure. These points of failure are often unique to every environment so we will cover these key points.

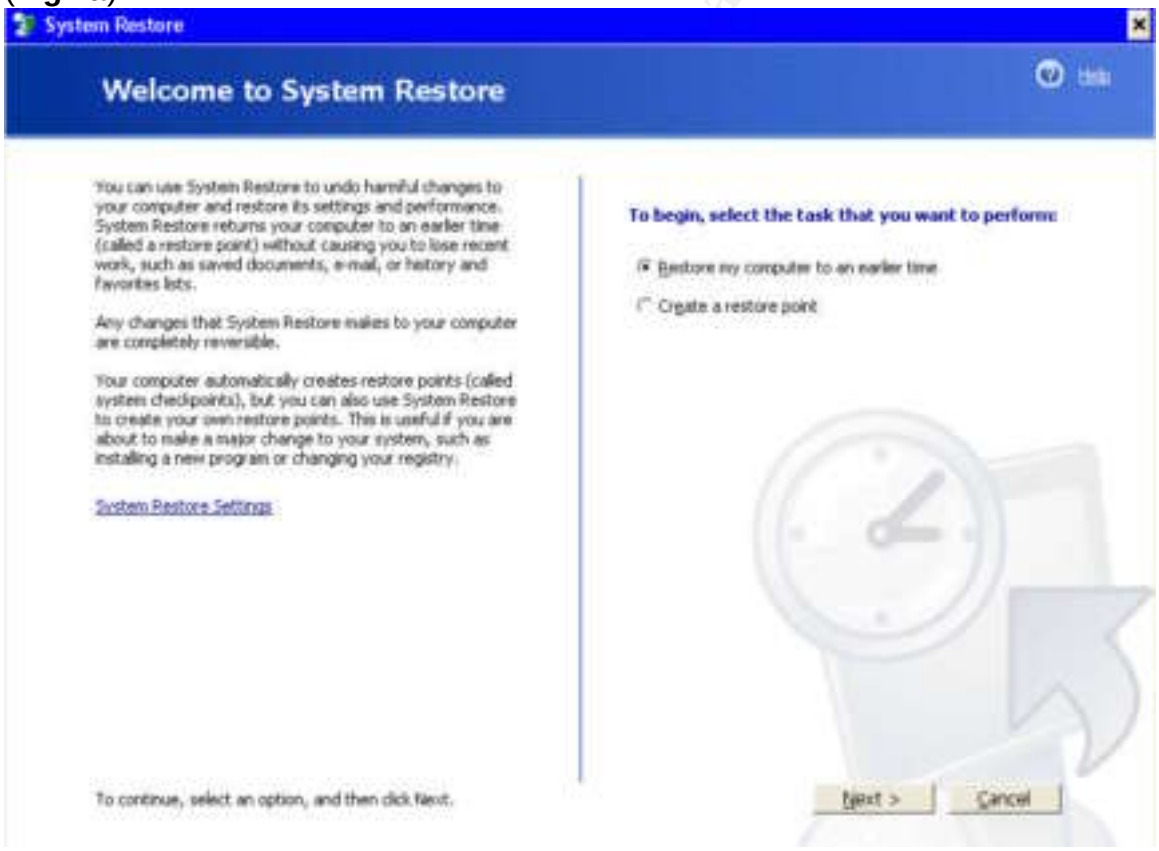
- Software
  - Windows XP Professional by Microsoft
  - Symantec Antivirus Corporate Edition by Symantec
  - Symantec Ghost by Symantec
  - Veritas Backup Exec 9.1 by Veritas

- Hardware
  - Raid 1 Capable Motherboards featuring Intel's 875P chipset.
  - External Hard Drives by Iomega
  - Uninterruptible Power Supply by APC

Software

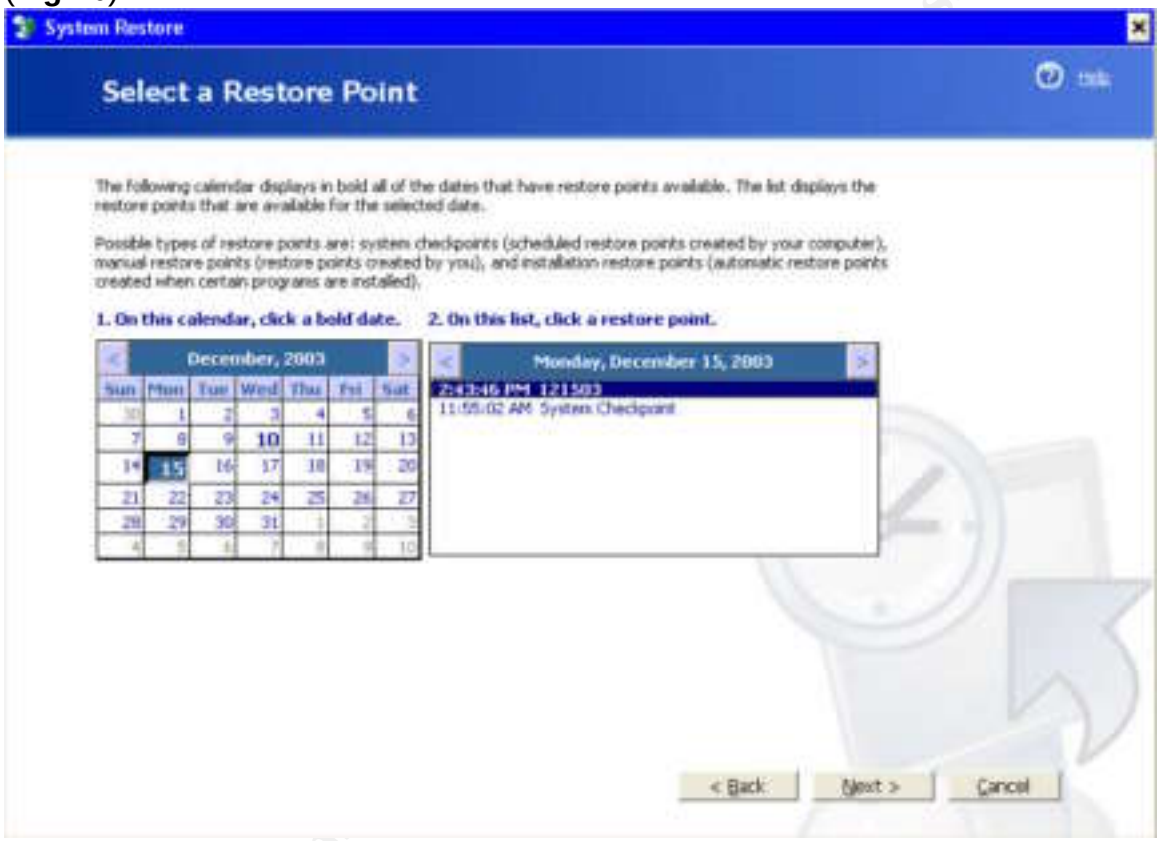
Microsoft Windows XP Professional

Software is often a point of failure but it can also be a means of recovering from a system failure. Microsoft Windows XP Professional is one such product. Windows XP Professional has built in redundancy in the form of an application called System Restore. System Restore can be found in Start, Programs, Accessories, System Tools, and left clicking on System Restore. This application is often overlooked by Network and Systems Administrators and can often recover a system that is giving a BSOD (Blue Screen of Death) when all other means fail. Blue Screens of Death are often caused by a corrupt registry. A corrupt registry can be caused by any number of things such as a user installing an inappropriate driver. The screen below shows the options that are available from System Restore.
(**Fig.1a**)



It is recommended to use the “Create a restore point” option after every new install even though this process of creating restore points is done automatically by Windows XP Professional if System Restore is turned on. System Restore can be turned on and off through System Restore tab in System Properties applet. This way, at the very least, the Administrator can get a system back up without having to install Windows XP Professional in its entirety and every

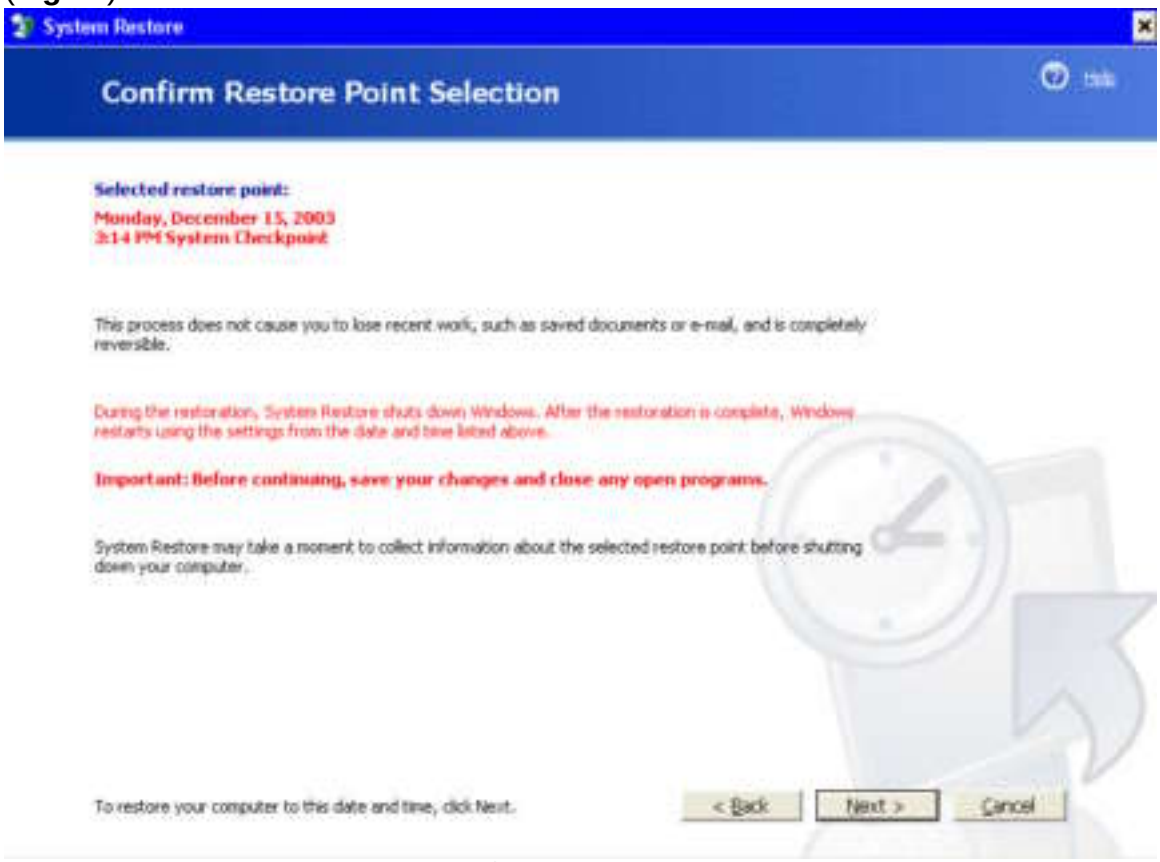
application that is applicable to the user. The Administrator can also be sure that it is a good restore point and not one that was automatically created by the failing Windows XP Professional operating system. The Administrator has the option when creating a restore point to name it, which is very helpful. Choose a name for the restore point that makes it easy to identify, by date would be an example, or any name that makes it easy to identify as to when the system was operating properly. Granted the application shows the Administrator when the restore point was created. The Screen below illustrates the options available.
(**Fig.1b**)



Note that the calendar in the above example displays dates in bold that contain restore points. Also notice the names, dates and times that are in the restore list. In the example above notice that December 10th is bold indicating that it contains a restore point. December 15th in the above example is selected, and contains two restore points, one created by the system and one created by the user.

To restore a system using the System Restore utility that will not boot normally, do the following. Boot to safe mode and open the System Restore applet by following the instructions provided earlier. Click on “Restore my computer to an earlier time” radio button as seen in figure 1a which will bring the user to the next screen as seen in figure 1b. Select the restore point suspected to be stable and click next. This will bring the user to the next screen seen on the following page as figure 1c. Note that the process is reversible. Click next. The system will restart and restore to the restore point specified.

(**Fig.1c**)



System Restore is not without its draw backs and has failed Administrators before in their time of need. If the Administrator receives a restore not successful message and the Administrator is not able to restore the system as described the Administrator can try the following manual method. This is a way to manually restore a system and is to be used at the users own risk and should only be used by those familiar with a command line interface. This is in no way guaranteed to work, however it does work for systems when GUI method proves unsuccessful. Note that following instruction is taken from a *part* of Microsoft Knowledge Base Article – 307545: and is not kb307545 article in its entirety. The following steps have been modified to reflect whereas booting to safe mode and using System Restore is not successful. Circumstances where safe mode is not an option is an indication that necessary system files have been damaged. Article kb307545 refers to a system where not even safe mode is available and requires the Administrator to recover files that were created during the initial install of Windows XP Professional. Microsoft Knowledge Base Article – 307545, Part 2, Section 2, 1-11, and Part 3, 1-3 provides the following instruction.

1) While still in safe mode and logged on as a user with administrative rights, start Windows Explorer.

2) On the Tools menu, click **Folder Options.**
3) Click the **View** tab.
4) Under **Hidden files and folders**, click to select **Show hidden files and folders**, and then click to clear the **Hide protected operating system files (Recommended)** checkbox.
5) Click **Yes** when the dialog box is displayed that confirms that you want to display these files.
6) Double-click the drive where you installed Windows XP to get a list of the folders. If is important to click the correct drive.
7) Open the System Volume Information folder. This folder appears dimmed because it is set as a super-hidden folder. Note that this folder contains one or more _restore {GUID} folders such as "_restore{87BD3667-3246-476B-923F-F86E30B3E7F8}".
8) Open a folder that was not created at the current time and that you suspect contains uncorrupted data. You may have to click **Details** on the **View** menu to see when these folders were created. There may be one or more folders starting with "RP*x* under this folder. These are restore points.
9) Open one of these folders to locate a Snapshot subfolder; the following path is an example of a folder path to the Snapshot folder: C:\System Volume Information_restore{D86480E3-73EF-47BC-A0EB-A81BE6EE3ED8}\RP1\Snapshot
10) Create a folder called “Tmp” in C:\Windows and from the Snapshot folder, copy the following files to the C:\Windows\Tmp folder:

    - REGISTRY_USER_.DEFAULT
    - REGISTRY_USER_.SECURITY
    - REGISTRY_USER_.SOFTWARE
    - REGISTRY_USER_.SYSTEM
    - REGISTRY_USER_.SAM

11) Rename the files in the C:\windows\Tmp folder as follows:

    - REGISTRY_USER_.DEFAULT to DEFAULT
    - REGISTRY_USER_.SECURITY to SECURITY
    - REGISTRY_USER_.SOFTWARE to S OFTWARE
    - REGISTRY_USER_.SYSTEM to SYSTEM
    - REGISTRY_USER_.SAM to SAM

12) Boot to the recovery console. This process can be done in one of two ways. The first way is done by booting your PC with your Windows XP Professional CD and choosing the Recovery Console option. The second way is selecting the Recovery Console Option from a boot menu. This option will not be available unless an Administrator or someone else has installed the Recovery Console. In order for this option to be available from a boot menu a user would have to install the Recovery Console on a PC before the user actually needs it. To install the Recovery console do the following. Click Start then Run and type [CDROM Drive letter]\i386\winnt32 /cmdcons and click OK and follow the instructions while Windows XP Professional is running. When running the Recovery Console the user must log on as administrator or as a user with administrative rights. (http://www.microsoft.com/windowsxp/pro/using/howto/gettingstarted/guide/backup.asp)

13) At the command prompt, type the following lines, pressing ENTER after you type each line:

```
copy c:\windows\system32\config\system c:\windows\tmp\system.bak
copy c:\windows\system32\config\software c:\windows\tmp\ software.bak
copy c:\windows\system32\config\sam c:\windows\tmp\ sam.bak
copy c:\windows\system32\config\security c:\windows\tmp\ security.bak
copy c:\windows\system32\config\default c:\windows\tmp\ default.bak
delete c:\windows\system32\config\system
delete c:\windows\system32\config\software
delete c:\windows\system32\config\sam
delete c:\windows\system32\config\security
delete c:\windows\system32\config\default
copy c:\windows\tmp\system c:\windows\system32\config\system
copy c:\windows\tmp\software c:\windows\system32\config\ software
copy c:\windows\tmp\sam c:\windows\system32\config\ sam
copy c:\windows\tmp\security c:\windows\system32\config\ security
copy c:\windows\tmp\default c:\windows\system32\config\ default
```

Note This procedure assumes that Windows XP is installed to the C:\Windows folder. Make sure to change C:\Windows to the appropriate windows_folder if it is a different location.

14) Type exit to quit recovery Console. Your Computer restarts.(http://support.microsoft.com/default.aspx?scid=kb;EN-US;307545)

Note that in step number thirteen we created a copy of the registry files in C:\Windows\Tmp so that we can get back to last state the system was in. It is a good practice to always have a way to get a system back to the original state

even if that state is corrupt. This allows for a process of elimination by trial and error and eliminating that what the Administrator changed did not make a problem situation even more complicated.

Sometimes corruption occurs to a specific user profile. An example would be errors or problems that are unique to that user when they logon to the PC but are not present when logged on as an Administrator or as another user. Here is a method that is often successful. If the only accounts are the corrupted account and the Administrator account, then the Administrator will need to create a new account to copy from. The Administrator can not make a copy of a folder containing profile information of an account he or she is logged on as. Create an account named "TestUser". If it is necessary to create a new account, logon to PC with this account after it is created in order to create a clean profile and then logoff, if there are already multiple user accounts on the PC that are stable, this step is not necessary. Logon to the PC as administrator and open Windows Explorer and browse to C:\Documents and Settings. Be sure that hidden files are being displayed by clicking Tools, Folder Options, and click on the View tab and select show hidden files. Note that there is a folder called Default User that is off color from the other folders. This off color is due to it being a hidden folder. When Windows XP Professional is first installed the Default User profile is created. Each new user that is created thereafter is built or copied from this default profile when they logon to the workstation or domain for the first time. The Administrator may have several folders that have names reflecting the names of user logon accounts of the users that have logged on to this PC. These folders hold user profile information and contain the information specific to that user. Examples would be desktop settings, temporary internet files, browser history, start menu, and application data such as user's Microsoft Outlook mailbox (*.pst file). First rename the problem account's folder. Do not delete this folder! An example would be renaming "username" to "usernameold". Make a copy of a working account folder or the one created by logging in as "TestUser" at the beginning of this lesson. Right click on the folder of choice and choose copy then right click in the C:\Documents and Settings folder and choose paste. This will create a folder named Copy of [folder name] in the C:\Documents and Settings folder. Then rename the "Default User" folder to "_Default User". Then rename the folder that has been copied to "Default User". An example would be renaming "Copy of TestUser" to "Default User". Logoff and have the user with the corrupt profile log in using their logon name. The user will create a new user profile in doing so; built from the Default User profile just created. All personal settings that were related to this user's account will be lost. These lost settings will include desktop settings and local email accounts as an example. The good news is that the reinstall of any applications or Windows XP Professional will not be necessary! Logon as Administrator and copy any missing files that were unique to that user and are not corrupted to the rebuilt account. Be sure to delete the Default User folder that was created and rename "_Default User" to "Default User".

There are two more items worth mentioning that are a lot less work. The first is using the F8 option at boot up and selecting "Last Known Good

Configuration". The F8 option rarely works, but is a lot easier than what has been covered thus far. The reason this option seldom works is because the "Last Known Good Configuration" uses a backup of the registry that was saved from last shut down. If the machine has been repeatedly shutdown and restarted before the Administrator is informed of a problem, the backup is of a corrupt registry and is no longer of any use. The second is a little utility built into the operating system called "sigverif.exe".
(http://support.microsoft.com/default.aspx?scid=kb;en-us;316434#23)
This utility verifies that the drivers have been tested by Windows Hardware Quality Labs and will allow the Administrator to identify drivers that have not been digitally signed by Microsoft. This does not mean that if this utility can not find any unsigned drivers on the system, the system does not have any unsigned drivers installed. Companies are constantly finding ways to deceive the operating system and the user. Use this utility as a tool to help troubleshoot these problems. The Administrator can move drivers that the utility identifies as unsigned to another directory in order to ascertain whether the unsigned drivers are the cause of the problem. Remember to never delete anything while troubleshooting, move the file or folder or rename it. Process of elimination is the best way to troubleshoot a problem. You may remember reading earlier how drivers, incorrect or corrupt, can crash a system. The Administrator can run this utility by clicking Start, Run, and typing sigverif and clicking OK. When the application starts notice three buttons, start, close, and advanced. Click on the advance button and then click on the browse button and browse to the %Windir%\System32\Drivers folder. The drivers in this folder are the only ones that need to be scanned in order to achieve a clean boot as per kb316434. This concludes the Windows XP Professional Operating system portion.

Virus Protection by Symantec

Virus Protection is a very important part of keeping a system highly available today. We all have seen the havoc that viruses and worms can reap on a network. In the case of the Slammer worm it only takes one machine to be infected to take down an entire LAN. Virus Protection applications rely on application updates so they are able to detect new viruses. Keeping a virus protection application up to date is not to be trusted to an end user and should only be the responsibility of Systems and Network Administrators. There are many virus protection products on the market today. It has been found all of the virus protection products on the market today tend to be comparable and very good at detecting viruses as long as their virus definition files are kept up to date. Symantec is one company of many that offers an anti virus product for corporate use called Symantec AntiVirus Corporate Edition. This product is easily configurable and is able to push these virus updates, as well as the client application, straight out to the desktop from the server. The Administrator is able to control what setting(s) the user can change or not. An example would be to not allow a user to scan network drives for viruses but do allow the user to scan floppy drives and CD's. The Administrator can prevent the user from disabling

virus protection altogether or the Administrator can set a time threshold, for example of five minutes; when five minutes has passed the virus protection is enabled again. This can be a very handy tool to protect those users that don't have to obey the rules. The antivirus server can also send the Administrator an email, a network broadcast message, or even page the Administrator if any of the desktop clients detect a virus. The Administrator can have the antivirus server check for updates from what Symantec calls Intelligent Updater. (http://service1.symantec.com/SUPPORT/sharedtech.nsf/d3c44a1678bd8f45852566aa005902cb/5f023692186abb02c1256b7200473ac3?OpenDocument&src=bar_sch_nam)
These virus definitions differ slightly from the LiveUpdate feature. LiveUpdate virus definitions are only updated weekly unless there is an alert situation. Intelligent Updater virus definitions are updated daily Monday through Friday. The difference to the Administrator is LiveUpdate can be scheduled through Symantec AntiVirus Corporate Edition but the updates are typically only released once a week. Intelligent Updater can be set up to run through a batch file which the Administrator can schedule to run via windows task scheduler, and the updates are available on a daily basis. Below is an example of the batch file and script one could use from Symantec's website. Both the batch file and script need to be copied to the folder that contains the application. Document ID: 2002091816510548; from Symantec's website offers the following script and batch file for download in addition to instructions for their use.

```
Batch file:
ftp -s:cescript.txt
c:\temp\symcdefsx86.exe /q
del "c:\temp\symcdefsx86.exe"
Script:
open ftp.symantec.com
anonymous
nobody@spammer.com
cd public/english_us_canada/antivirus_definitions/norton_antivirus/static
lcd C:\temp
bin
hash
prompt
get symcdefsx86.exe
quit
```

(http://service1.symantec.com/support/ent-security.nsf/docid/2002091816510548?Open&src=bar_sch_nam&docid=2002021908382713&nsf=sharedtech.nsf&view=d3c44a1678bd8f45852566aa005902cb&dtype=&prod=&ver=&osv=&osv_lvl)

Application and system patches are crucial to preventing viruses and should be kept up to date and not trusted to the end user. Many viruses like the slammer worm are made to exploit known security holes in systems that have not been

patched. This is why virus protection and patch management need to addressed as a whole.

Backup Solutions by Veritas Backup Exec 9.1
Imaging Software by Symantec Ghost

There are ways of protecting the executives PC's from even the worst viruses, the most corrupt operating system, and unrecoverable hardware failure and that is what will be addressed next. Imaging software such as Symantec Ghost and back up software like Veritas Backup Exec 9.1 make a very good partnership for such redundancy. By using Imaging software the Administrator is able to make an exact copy of all data including the operating system and all applications.
(http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=3)
Combining this Ghost image with an application like Veritas Backup Exec enables the administrator to restore the executive's PC's in a relatively short amount of time even with a complete hardware failure. With Veritas Backup Exec 9.1 the Administrator can backup the executive's files for them. It is not advisable to do so without telling them however. With Veritas Laptop and Desktop Agent the Administrator is able to push the client application out to the user.
This makes it very easy to administer. The Administrator can even give executives the choice to synchronize or merge data on their PC or laptop with a server share or data on the server share with their PC or laptop. This synchronization can be very useful for traveling executives or in times of crisis. Even the most apprehensive of executives will get peace of mind knowing that their data is protected with 128 bit AES encryption at the file level as claims Veritas.
(http://eval.veritas.com/downloads/pro/backup_exec/bews_91_dlo_opt_wp.pdf)

Hardware

Intel's 875P Chipset

With today's technology there are new forms of hardware redundancy that are very affordable. The Administrator can now offer RAID 1 reliability to the executives without expensive hardware such as SCSI controllers. The latest motherboards from Intel, featuring the 875P chipset boast dual serial ATA (Serial Advanced Technology Attachment) controllers on board. This allows for a RAID configuration of RAID 0 or RAID1.
(http://www.intel.com/design/chipsets/875P/875P_PB%208.pdf)
RAID 0 and RAID 1 requires at least two disks. RAID 0 offers no redundancy and does not apply to this subject. RAID 1 is also known as disk mirroring and provides redundant data because of the fact that the data is written to at least two disks. These disks are an exact copy of each other. Read performance

increases because these disks can be read simultaneously. There is no performance increase in writing data however. If one disk were to fail, the Administrator has an exact copy of that data on the other disk(s). This is useful for hardware failures, but in the event of operating system corruption, both disks would share the corruption. This is why hardware RAID is preferred over so called software RAID. Software RAID is controlled by an application. If the application the controls the RAID becomes corrupt the whole system is inaccessible. (http://www.pcguide.com/ref/hdd/perf/raid/conf/ctrlSoftware-c.html)

Iomega HDD 250GB USB 2.0/FireWire External Desktop Hard Drive
Iomega features very fast 7200 rpm external hard drives that are highly reliable. The Iomega HDD 250 includes Symantec Ghost 2003 and Iomega Automatic Backup giving the Administrator or the technically savvy executive, the ability to create an image of an executive PC, back up data from the executive PC, and the ability to run applications from the external hard drive. It has USB 2.0 and FireWire interfaces and works with any Operating System from Windows 98 to XP. This means that the executive can merely take his or her work home with him or her and attach it to whatever Operating System he or she is running at home. The unit is small enough to store in a fire proof safe so that the Administrator could have one for every high level employee in his or her place of business.
(http://www.iomega.com/direct/products/detail.jsp?PRODUCT%3C%3Eprd_id=8318797&FOLDER%3C%3Efolder_id=58741&ASSORTMENT%3C%3East_id=67&bmUID=1071901344400)

Uninterruptible power Supply by APC

In order for a PC to be highly available it definitely needs power. Most companies that realize the importance of their computer systems have generator back up. But sometimes generators fail or do not start up in time to keep a PC from powering down unexpectedly. This unexpected power loss can result in data loss and damage to the PC. That is why executive PC's and all PC's for that matter should be protected by a UPS. A UPS does more than just provide power in the event of complete power loss. UPS's protect a PC from drops in power called brown outs and spikes in power called power surges and provide consistent clean power for the PC. Some UPS's provide protection for Ethernet and or modems by providing the appropriate pass-through ports. In the event of a lightning strike it could save a PC that might be vulnerable from electrical discharge that could occur via the Ethernet cable or phone line. APC has a software product they call PowerChute that will log these brownouts and spikes and some models alert the Administrator via a popup menu or network broadcast message to inform the Administrator of these outages and spikes. PowerChute will also safely power down the system before battery dies when on battery power. In the event of a power loss the UPS will produce an audible beep to tell the user there has been a loss of power. This should be an alert to

the user to power down the PC safely and to save their work. It does not mean to continue working until the generator kicks in. (http://www.apc.com/products/)

Conclusion

The best way to get executive staff on board with the company policies is educating them on the ramifications of their actions and making the path to compliance an easy one. Do not fear these Executives or assume they do not care. The information preceding this conclusion is an example of the extra steps necessary in order to provide this high availability for Executives. Many of these steps would not be necessary if everyone followed the same policy. Policies that are clear and concise are the key to nirvana. Remember a chain is only as strong as its weakest link.

References

Microsoft. "How to Recover from a Corrupted Registry That Prevents Windows XP from Starting." 12 Dec. 2003 http://support.microsoft.com/default.aspx?scid=kb;EN-US;307545 (18 Dec. 2003)

Microsoft. "Back Up and Recover Your Information." (24 Aug.2001) http://www.microsoft.com/windowsxp/pro/using/howto/gettingstarted/guide/backup.asp (17 Dec. 2003)

Microsoft. "HOW TO: Perform Advanced Clean-Boot Troubleshooting in Windows XP." How to Remove Unsigned Drivers. 4 Nov. 2003 http://support.microsoft.com/default.aspx?scid=kb;en-us;316434#23 (11 Dec. 2003)

Symantec. "LiveUpdate." knowledge base. 19 Feb. 2002. http://service1.symantec.com/SUPPORT/sharedtech.nsf/d3c44a1678bd8f45852566aa005902cb/5f023692186abb02c1256b7200473ac3?OpenDocument&src=bar_sch_nam (9 Dec. 2003)

Symantec. "How to automatically update Symantec AntiVirus Corporate Edition 8.x definitions without using LiveUpdate" Document ID: 2002091816510548. 12 Aug. 2003. http://service1.symantec.com/support/ent-security.nsf/docid/2002091816510548?Open&src=bar_sch_nam&docid=2002021908382713&nsf=sharedtech.nsf&view=d3c44a1678bd8f45852566aa005902cb&dtype=&prod=&ver=&osv=&osv_lvl
(1 Dec. 2003)

Symantec. “Symantec Ghost Corporate Edition.”
http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=3
(11 Dec. 2003)

Veritas. “Data Protection and Synchronization for Desktop and Laptop Users.”
http://eval.veritas.com/downloads/pro/backup_exec/bews_91_dlo_opt_wp.pdf
(18 Dec. 2003)

Intel. “Intel 875P Chipset Product Brief.”
http://www.intel.com/design/chipsets/875P/875P_PB%208.pdf
(18 Dec. 2003)

http://www.pcguide.com/ref/hdd/perf/raid/conf/ctrlSoftware-c.html
(17 Dec 2003)

http://www.iomega.com/direct/products/detail.jsp?PRODUCT%3C%3Eprd_id=8318797&FOLDER%3C%3Efolder_id=58741&ASSORTMENT%3C%3East_id=67&bmUID=1071901344400
(18 Dec 2003)

http://www.apc.com/products/
(11 Dec 2003)