



System and Data Security

Contents

| | |
|---|----|
| Foreword | 1 |
| What this document will do for you | 1 |
| Tape Backups | 2 |
| Type | 2 |
| Cycle | 2 |
| Selection list | 4 |
| Storage of media | 4 |
| Integrity | 4 |
| Cleaning and media lifetime | 5 |
| Test restoration | 5 |
| Damaged media | 5 |
| File Backups | 6 |
| Archiving file based backups | 6 |
| System and Data Security | 7 |
| Password Policy | 7 |
| Screensaver/Unattended workstation Policy | 7 |
| Off-Site Data | 7 |
| Equipment Disposal | 7 |
| System Integrity | 8 |
| Viruses, Trojans, Adware and Tracking Cookies (Spyware) | 8 |
| Anti-Virus Software | 9 |
| Security Flaws and Patches | 10 |
| Hackers, Backdoors and Firewalls | 11 |
| System Resilience | 13 |
| Hardware Warranty | 13 |
| Maintenance | 13 |
| Power | 14 |
| Disk Space | 15 |
| Equipment Location | 15 |
| SIMS .net SQL Database | 16 |
| Backing up SQL | 16 |
| Database Size | 16 |

Foreword

This document describes aspects of computer systems that are often overlooked or taken for granted by many users. I cannot stress enough, the importance of data security. You can take my word for it that in the event of a computer failure or theft, data security will be in the forefront of your mind.

It is all too easy to put off or ignore security and disaster recovery issues. These are not areas that affect you frequently, but when they do it normally hurts, both financially and mentally!

How business critical is your computer system? If you cannot function without it, take appropriate steps to put in place some sort of fail-over. This can be as simple as reverting to paper based records, or as complicated as another computer to replace a core system in the event of failure.

More often than not, data is permanently lost due to small oversights or assumptions – most of which could have been corrected if the right questions had been asked earlier, and simple day to day management tasks had been performed.

What this document will do for you

This document is intended to give you a pointer to things you should consider, and a general overview of what is possible. It won't give you step by step instructions for implementing the topics covered – it is simply not possible to document every possible scenario in enough detail.

Capita can provide consultancy services to discuss your particular requirements in more detail, and we can in many cases implement changes to your computer systems to make things easier. What we can't do is manage your system on a day-to-day basis. This is something you must do.

If you don't have the expertise, Capita can also provide an On-Site Support Service. The On-Site Support Service gives you an expert for a fixed number of days over a year. They can keep an eye on things for you, suggesting and implementing changes as agreed with you. Again, this is no substitute for good day-to-day management, but it does give a form of compromise.

Tape Backups

Backing up data to off-line storage is one of the most important and often overlooked aspects of any computer system. In the event of fire, theft, or hardware failure, an off-line backup may be the only source of recoverable data. You own the data and as such can be the only people responsible for ensuring its security.

All too often backups are taken for granted. This mistake is normally discovered when you lose everything – and once you lose it, you can't get it back! Remember that no-one else will be affected by your loss. For you however, it may have devastating and far reaching consequences.

To put this rather grim scenario in context, imagine trying to recreate your finance records from scratch for the last financial year, then consider the problems you will have reconciling at end of year. Not a pleasant thought is it! Not only unpleasant, it is an expensive and stressful process for the staff involved.

The other consideration for backups is the possible need to restore data that has become corrupt. Sometimes this corruption can go undetected for a period of time. The number of archive backups you hold becomes important in this situation. If you don't discover a problem for two weeks, which tape can you restore from? With a normal backup cycle of [Mon-Fri, Spring, Summer, Autumn], the last termly tape will be the only one available. This could be many months old.

Type

Avoid Differential, Incremental and Partial backups wherever possible. These methods rely on multiple tapes to initiate a restoration. If one of these tapes is missing or damaged, you cannot restore.

In the scenario where the amount of data you backup is greater than the tapes capacity, your first consideration should be to replace the tape drive. If this is not possible, selected items can be removed from the daily backup – but it must be remembered that in the event of a restoration, this may delay the process or limit what can be restored. It may also incur cost for re-installation.

It may seem expensive to replace the tape drive, but in the long run you will make savings if you ever need to rely on it for data recovery.

Capita recommends

Perform a Full daily backup. If your data won't fit onto one tape, purchase a larger capacity tape drive.

Cycle

Daily backups should be taken using a sensible media rotation cycle.

You can use one of several rotation cycles using a varying number of tapes. The general rule of thumb is "the more tapes you use, the less data you lose".

Capita supply standard systems with eight tapes. This is the minimum recommendation for a backup cycle. We would recommend using more tapes wherever possible.

Some different rotation methods are outlined on the following page.

| Termly Rotation | | | | | |
|--------------------------|---|-----|-----|-----|--------|
| Media Qty Required | 8 | | | | |
| Daily Media | Mon, Tue, Wed, Thu, Fri | | | | |
| Archive Media | Spring, Summer, Autumn | | | | |
| Restore Points | Any day over the last week, one day in the previous three terms | | | | |
| Rotation Cycle | | | | | |
| Week 1 | Mon | Tue | Wed | Thu | Fri |
| Week 2 | Mon | Tue | Wed | Thu | Fri |
| ... | ... | ... | ... | ... | ... |
| Last week of Spring term | Mon | Tue | Wed | Thu | Spring |
| Last week of Summer term | Mon | Tue | Wed | Thu | Summer |
| Last week of Autumn term | Mon | Tue | Wed | Thu | Autumn |

| Simple Grandfather-Father-Son | | | | | |
|--------------------------------------|---|-----|-----|-----|--------|
| Media Qty Required | 10 | | | | |
| Daily Media | Mon, Tue, Wed, Thu, Fri1, Fri2, Fri3 | | | | |
| Archive Media | Spring, Summer, Autumn | | | | |
| Restore Points | Any day over the last week, the previous three Fridays, one day in the previous three terms | | | | |
| Rotation Cycle | | | | | |
| Week 1 | Mon | Tue | Wed | Thu | Fri1 |
| Week 2 | Mon | Tue | Wed | Thu | Fri2 |
| Week 3 | Mon | Tue | Wed | Thu | Fri3 |
| Week 4 | Mon | Tue | Wed | Thu | Fri1 |
| ... | ... | ... | ... | ... | ... |
| Last week of Spring term | Mon | Tue | Wed | Thu | Spring |
| Last week of Summer term | Mon | Tue | Wed | Thu | Summer |
| Last week of Autumn term | Mon | Tue | Wed | Thu | Autumn |

| Complex Grandfather-Father-Son | | | | | |
|---------------------------------------|--|------|------|------|----------|
| Media Qty Required | 24 | | | | |
| Daily Media | Mon1, Tue1, Wed1, Thu1, Fri1, Mon2, Tue2, Wed2, Thu2, Fri2, Fri3 | | | | |
| Archive Media | Period 1, Period 2, Period 3, Period 4, Period 5 ... Period 13 | | | | |
| Restore Points | Any day over the last two weeks, the Friday before, any fourth Friday before | | | | |
| Rotation Cycle | | | | | |
| Week 1 | Mon1 | Tue1 | Wed1 | Thu1 | Fri1 |
| Week 2 | Mon2 | Tue2 | Wed2 | Thu2 | Fri2 |
| Week 3 | Mon1 | Tue1 | Wed1 | Thu1 | Fri3 |
| Week 4 | Mon2 | Tue2 | Wed2 | Thu2 | Period1 |
| ... | ... | ... | ... | ... | ... |
| Final week of year | Mon2 | Tue2 | Wed2 | Thu2 | Period13 |

Archive media should be kept indefinitely. Remember to purchase additional archive media each year, and to replace daily media as per manufacturer's lifetime recommendations.

Capita recommends

Perform the most complex media rotation cycle you can afford – the more archive tapes you use, the more restore points are available to you.

Selection list

Your backup job should be configured to backup all files on all fixed disks – normally C: and D:

Don't backup the CDROM, Substituted or Network drives – normally P:, O:, R:, S: and X:

Ensure System State or Volume Shadow Copy is selected if listed. This contains all the vital files the operating system needs to operate, as well as the configuration of your network.

Microsoft SQL as used by SIMS .net has specific issues which are outlined in the SQL section later in this document.

Capita recommends

Ensure your selection list includes all files on all fixed disks and ensure System State or Volume Shadow Copy is selected if listed.

Microsoft SQL has specific issues as the database is always in use, and cannot therefore be backed up without taking appropriate steps. See the SQL section later in this document for recommendations.

Storage of media

Backup media should be stored in multiple secure locations.

There is little point religiously taking daily backups and checking your logs, then leaving all the tapes next to the fileserver. If it is stolen, the tapes may be taken as well. Likewise, don't leave all the tapes in the same building. If it burns down, or suffers flood damage, the tapes are unlikely to survive.

The most bizarre incident I have seen involving location of tapes was due to asbestos. Once identified, the contents of the building were condemned and everything was incinerated! The only source of data was an archived tape from several months earlier that had been kept off site.

Capita recommends

Take the last good backup off-site overnight and return it the following day. Keep the tape before that off-site until the following day. In other words...

On Thursday afternoon take home the Wednesday and Tuesday tapes. Leave the Tuesday tape at home. On Friday morning, return the Monday and Wednesday tapes to the office.

On Friday afternoon, take home the Thursday and Wednesday tapes. Leave the Wednesday tape at home. On Monday morning, return the Tuesday and Thursday tapes to the office.

This allows a compromise between the possible need to restore data from yesterdays backup against the loss of one days work should this tape be destroyed during the day, or in an accident on the way to work – this may seem morbid, but scenarios like this are possible, so should be considered

Integrity

Check your backup logs every day. And don't make the mistake of simply looking at the completed status, "Completed successfully" doesn't mean all your data has been backed up.

If software is left running overnight, there is a chance that files are held open and cannot be read by the backup software. If you find yourself in this scenario, keep an older tape that does have a complete backup with the latest tape that you take off-site.

You will need to get a feel for what your daily backup logs look like before you start to notice irregularities. You may find that a good backup will have some files that were unable to be backed up. Various files are held open by the Operating System during its normal use. These files are usually backed up by the Operating System itself, so the backups the Operating System makes will be on tape, but not the live files.

There are scenarios where files added to the system are excluded from the backup until the selection list is modified. Periodically check the selection list on your overnight backup job. All files on all fixed disks should be selected, and System State or Volume Shadow Copy should also be selected if listed.

Capita recommends

Start by ensuring you have a good backup in the first place.

If you aren't sure how to interpret the logs, fax or email a copy of your first log to the Capita HelpDesk. Capita can advise you if your backup is good or not. Once this is confirmed, you should look for changes in future during your daily backup log check.

Cleaning and media lifetime

It is very important that tape drives are maintained in working order by running a cleaning tape in accordance to the manufacturers' recommendations.

Every time you run a backup, some of the tape surface will be left on the tape drives recording and play heads. Eventually, this will cause problems reading and writing to tapes.

Dirt and dust is also drawn into the tape drive from the tapes themselves, and by the computers in-built cooling fans.

All recording media has a limited lifetime of use. Tapes beyond their lifetime should be discarded and replaced with new ones according to manufacturers' recommendations.

In line with the System and Data Security section later in this document, you should destroy old media properly. Don't throw old tapes in the bin; anyone could use the tape to restore confidential and sensitive information. Either incinerate or de-spool the tape and cut it into pieces by passing it through an appropriate shredder.

Some recommendations for various manufacturers' drives and media:

| Media Type | Tape Lifetime | Cleaning Cycle |
|-------------------|-------------------------|---|
| HP Travan | 100 backups or 2 years* | Self cleaning |
| Seagate Travan | 100 backups or 2 years* | New Tapes: After 2 hours use Otherwise: Once a month |
| DAT | 100 backups or 2 years* | Once a week |
| DLT / SDLT | 100 backups or 2 years | As indicated by drive |
| Ultrium | 260 backups or 5 years | As indicated by drive |

*Note these differ from previous recommendations of annual replacement as tape manufacture has improved in recent years. Any Travan or DAT tapes manufactured before 2004 have a 1 year lifetime unless otherwise stated on the tape packaging

Capita recommends

Ensure you clean your tape drive and replace your media according to the manufacturers' recommendations.

Ensure you are using the correct cleaning cartridge. DLT1/VS80 tape drives use a specific cleaning cartridge that is different from other DLT drives.

Test restoration

Whilst everything may look like its working, there is the possibility that data cannot be read from backups at a later stage. Periodic test restorations can be performed to verify data can be recovered from tape.

Realistically, this isn't easy to achieve without a duplicate system – which most of us don't have.

A compromise would be to select a few files at random and restore them to a redirected location. Don't attempt to do this unless you know what you are doing, it is possible to stop your system working by getting this wrong.

Damaged media

Regularly check that your tapes are not damaged. Damaged tapes should not be used as they could damage the tape drive itself.

Discard damaged tapes and replace them with new ones immediately. Keep a stock of spare tapes for this purpose.

If you use Travan or DAT tapes, opening the flap should reveal tape going from one side of the spool to the other. DLT/SDLT or Ultrium tapes should only have a header loop visible.

File Backups

Whilst tape backups are ultimately your fallback in a disaster recovery situation, there are times where taking a file based backup is a more practical solution to an immediate problem. A situation where this would be sensible is before you perform a SIMS upgrade.

Taking a file based backup of SIMS before performing an upgrade allows you to recover more quickly if it fails.

Remember though; file based backups use up space on your hard disk and subsequently your tape backup. Don't keep file backups longer than you need to. Check your backup logs more carefully the next day to ensure it has not been affected by the increased size of data it is writing to the tape.

Archiving file based backups

If you think you may need a file based backup in future but can't afford the loss of disk space for a long time period, archive it to a backup tape and then remove it from the hard disk – it can easily be restored at a later date if needed.

Capita recommends

Before running a SIMS upgrade, stop the MSSQL\$SIMS service, then take a file backup of the S:\SIMS and D:\Microsoft SQL Server\MSSQL\$SIMS\Data folders to a suitably named folder under S:\. Once copied, restart the MSSQL\$SIMS service and then perform your upgrade.

Remember to ensure you have enough free disk space to copy the files, and to allow the upgrade to run.

If no problems surface in the next month, delete the file backup.

System and Data Security

Under the terms of the Data Protection Act, you are responsible for ensuring the security and validity of any data held.

This article describes some simple steps you can take to minimise data security issues.

Password Policy

Enforce a password change policy. This can be as simple as telling your staff to change their passwords regularly, or more efficiently by configuring security settings on your fileserver to force changes when necessary (note, this can only be performed for network login, not application software).

Use strong passwords, that is to say a mixture of upper and lowercase letters and numbers.

Don't use passwords that are easily guessable.

There are various default system accounts that may still have generic passwords. Changing these passwords will probably have a knock-on effect, so don't change them if you are unsure.

Capita recommends

Enforce strong password changes every 30 days, not allowing the previous three to be reused.

Change the default system account passwords to something more unique.

There is an obvious trade-off between Capita being able to provide instant support and you having unique passwords. If you wish to change these and are happy for Capita to know the default system account passwords, please let us know and we will keep a secure record for support purposes only.

Please remember, if we are unable to gain prompt access to a password, it may limit our ability to support you, and in some circumstances compromise the terms of your support contract.

Keep a record of your default system account passwords on a document in your safe.

Screensaver/Unattended workstation Policy

What happens when you walk away from your computer leaving it unattended?

It's the equivalent of leaving the keys in your car, the door open and the engine running. You wouldn't do it with your car, so don't do it with your computer!

Never leave a logged in workstation unattended. Lock the console when you walk away from the computer by pressing CTRL-ALT-DEL and selecting Lock Computer. When you need to unlock, press CTRL-ALT-DEL and type in your network login password.

Be careful who you allow to use your computer whilst still logged in as yourself. Each user on the network has specific access rights. You may be allowing someone to view things inappropriate to their level of access.

Capita recommends

Switch your screensaver on and enable the option to request a password on resume. Set it for a maximum of 10 minutes delay.

Lock the console when you walk away from the computer by pressing CTRL-ALT-DEL and selecting Lock Computer.

Don't allow others to use your computer unattended whilst still logged in as yourself.

Off-Site Data

Use common sense if data is taken off-site on laptops or tape media, ensure it is stored in a secure location.

Capita recommends

Don't leave tapes or computers in cars or other insecure locations overnight.

Equipment Disposal

What happens to all the sensitive data stored on your hard disk when you dispose of old equipment?

If you don't erase computer hard disks before disposing of them, anyone with a small amount of computer knowledge can easily retrieve personal data. If you don't know how to do it yourself, Capita provides a service to erase data as part of any installation we perform.

If you plan to re-use computers elsewhere, think carefully about what information is stored on the hard disks before relocating them. You may not realise it, but copies of documents you have opened are probably stored in 'cache' folders on the hard disk, even if the document you opened wasn't originally stored on this computer.

Capita recommends

Erase computer hard disks before disposing of them.

If planning to re-use computers elsewhere, erase the hard disk and re-install the Operating System and Application software before relocating.

System Integrity

Many schools are considering whole school networks. Whilst this may give advantages in the form of lower management costs, it can cause a nightmare from the point of view of security.

There will always be a minority of people that will attempt to hack into or damage the network in some way.

Limit access to data to those that need it. Use file/folder security and group membership to set explicit security restrictions.

Joining your admin network to the curriculum network should be treated the same way as plugging your network directly onto the Internet without a firewall (see the section below about firewalls). Both locations will potentially have people trying to attack and compromise the security of your systems.

Don't confuse the need for access to SIMS from the curriculum network with the need for a whole school. More often than not, configuring a trust relationship between the two networks is sufficient. If you are unsure what you need to do, Capita can advise you what solutions will fit your business need.

Viruses, Trojans, Adware and Tracking Cookies (Spyware)

As we are all too aware, there are many viruses out there on the Internet just trying to get into your system. Unfortunately, the main reason virus infections occur is due to recklessness and a lack of security on behalf of users.

Viruses and Trojans are applications that cause damage to your computer, or others computers by executing from your computer.

Adware is advert supported software. Periodically, adverts will popup on the screen causing annoyance and are frequently pornographic in nature.

Tracking Cookies track your use of the internet and the pages you visit. This information is sent to others for unknown purposes.

Viruses spread by various methods including email, port scanning, open shares, insecure passwords and security flaws in the Operating System or application software. Security flaws are covered in a later section.

If aspects of your system are insecure, you leave yourself open to attack.

Remember the following rules whilst using the Internet:

- Don't click on links in emails unless you are absolutely sure the source of the email is valid. The link may look valid, but they can be spoofed – In other words it displays one thing on screen, but actually goes somewhere else when clicked.
- Don't visit web sites unless you are absolutely sure of the content. Adware and Tracking Cookies are mainly spread by downloading as part of a web page.
- Never click on an unexpected dialog that looks like a Windows dialog whilst navigating web pages. Press Alt-F4 to close any suspicious looking dialogs – never click on the buttons, they may look genuine but believe me they probably are not! You will either be installing Spyware, a Virus, or end up being redirected to a web page trying to sell you something.
- Don't open emails that you don't recognise. Simply by opening an email, you can install a malicious program on your computer.

- Be very careful opening any email purporting to come from a bank. 99.9% of these emails are malicious and ask you to visit a fake web site and pass on your security details. Official emails from banks are very unlikely to contain links to their web sites.
- Don't download and install software from unknown sources.
- Don't download and install software unless appropriate tests have been made on a non-critical computer.
- Only install software required for your business needs.

Capita recommends

Follow the rules above whilst using the Internet.

Perform regular scans on computers with either Ad-Aware (www.lavasoft.de), Microsoft AntiSpyware Beta (www.microsoft.com) or similar software. This software will scan you computer for Spyware and allow you to remove it.

Be careful though. If you have a malicious program installed that is replacing a core system file, you may render your computer unusable as you clean it.

Anti-Virus Software

I am always being asked "how did I get a virus? I'm running Anti-Virus software". You have to remember that Anti-Virus software will only detect known viruses on your computer; it won't necessarily stop you from getting them in the first place. If your Anti-Virus software isn't updating regularly, you leave yourself open to infection from new viruses.

New viruses are released all the time, and in some circumstances you may have an active virus on your computer already but not realise. Until your Anti-Virus software has received an update to detect a virus, it won't know about it. Just this scenario happened several years ago with the Nimda and Blaster viruses.

The Nimda and Blaster viruses spread so quickly around the Internet that a huge amount of computers became infected before Anti-Virus software manufacturers even knew the virus existed.

In the case of some recently prevalent viruses, it was actually worse than simply becoming infected with a virus. Many people were subsequently unable download updates for their Anti-Virus software. This was either due to the virus swamping their Internet connection whilst the virus was trying to infect others, or the Internet Service Provider having temporarily suspended the Internet link from infected site – in this scenario, you would need to obtain the relevant cleanup utility or virus update by using another Internet connection from an alternate location.

Due to the prevalence of viruses and ease at which you can become infected, Capita was forced to begin charging for all virus cleanups several years ago, so be careful – if you become infected and cannot remove the virus yourself, it can become expensive.

It is ultimately your responsibility to ensure that all reasonable steps are taken to avoid virus infection. As outlined above, it is still possible to become infected with a virus, but this will hopefully be in a minority of cases.

You can check the Symantec "Security Response" (<http://securityresponse.symantec.com>) and Network Associates "Virus Information Library" (<http://vai.nai.com>) web sites for information on viruses and spyware and how to remove it from your computer.

Capita recommends

Regularly check your Anti-Virus software to ensure it is updating.

Schedule a full system scan to run at least once a week. If this is not possible because you can't guarantee the computer will be switched on at the scheduled time, run it manually from time to time.

Removable media and 3rd party laptops

You may have your own computer systems covered, but what about home computers or visitors' computers?

If you regularly bring files from another location, consider performing a virus scan before copying files to your work computer.

If you work on your home computer, why not purchase a license to install on your home computer, thus ensuring it is protected to the same level as your work computer?

If you receive visitors that plug their laptops into your network, consider inspecting the computer for up-to-date versions of Anti-Virus software, or even perform a full virus scan before allowing them to plug in.

Capita recommends

Update your Anti-Virus software daily. Most networks will have a central location on the fileserver that auto-updates from the Internet. Network workstations in turn receive their updates from this central location as they log onto the network.

Standalones are normally configured to receive their updates from the Internet. It is important to ensure that the scheduled update time is during the day when the computer is actually turned on. Set it for early morning or mid-day.

Keep an eye out for unusual things happening on your computer. If an annoying window keeps popping up, or your computer crashes or reboots for no apparent reason, it is possible you are infected so seek help as soon as possible.

Remember that whilst Capita will charge you to clean a virus, we don't charge to identify if you are infected. We will examine your computer remotely and point you in the right direction if a virus is found.

Scan removable media if you bring files from off-site.

Scan visitors' laptops before allowing them to plug into your network.

Security Flaws and Patches

It's recently become a well publicised fact that security flaws exist in Microsoft Operating Systems and software. Due to the complexity and size of the code behind Operating Systems and application software, it is very unlikely that all security flaws are removed or even identified before being released. However, in an effort to remove these, Microsoft actively releases patches to overcome security flaws as they become apparent. They are usually released on Tuesdays nights – which incidentally, are known in the industry as "patching Tuesday's"!

You can subscribe to a notification service to be made aware of patches as they are released by visiting www.microsoft.com/security.

From time to time, these patches are amalgamated into a single update called a Service Pack. Service Packs not only patch security flaws, they often add new features so care should be taken when installing them.

Patches and Service Packs can be downloaded by visiting windowsupdate.microsoft.com.

If your computer is running Windows 2000, XP or Server 2003, there is a built in facility to download updates automatically. This is called "Automatic Updates" and can be found in Control Panel. Automatic Updates can be configured to download updates and then either install them at a predetermined time of day, or to prompt you to install them. The latter is the most effective as it allows you to have some control over what updates are installed – you can even reject an update if you wish.

Capita recommends

Regularly visit windowsupdate.microsoft.com to get the latest security updates for your Operating System.

If your computer is running Windows 2000, XP or Server 2003, configure Automatic Updates to download patches automatically and prompt you to install them.

Regularly visit office.microsoft.com to get the latest security updates for the Office suite of applications.

Patch management

For large networks, employing some form of patch management system will save you a lot of time and effort. There are various products on the market including offerings from Shavlik, Symantec and Microsoft.

Microsoft's product is limited in what it can do, but it is free. Windows Server Update Services (available from www.microsoft.com/wsus) will patch the Operating System, Office and many other Microsoft applications.

Patch management systems allow your fileserver to automatically download patches and Service Packs from Microsoft as they are released. You control whether these are then approved for distribution to your workstations. Once approved, workstations will automatically update themselves from files stored on your fileserver.

Despite the fact that patches and Service Packs are put through extensive testing by Microsoft and its partners, occasionally unforeseen problems do creep in. Therefore, it isn't good practice to update every computer with a new patch or Service Pack without testing it on a few first. WSUS will allow you roll out a patch to just a few computers.

Capita recommends

Install Microsoft Windows Server Update Services on your fileserver. This will allow you to centrally manage the process of patching workstations.

Current Service Pack versions:

| OS / Software | Service Pack |
|---------------|------------------|
| Windows NT4* | Service Pack 6a* |
| Windows 2000 | Service Pack 4 |
| Windows XP | Service Pack 2 |
| Windows 2003 | Service Pack 1 |
| Office 2000 | Service Pack 3 |
| Office XP | Service Pack 3 |
| Office 2003 | Service Pack 1 |

*As of April 2005, Windows NT is no longer supported by Capita

Hackers, Backdoors and Firewalls

For your computer to communicate with the Internet and indeed other computers, it has to transmit and receive data across a network. This leaves your computer open to being hacked from outside sources.

To limit the number of "backdoors" available to hackers, you need to employ what is known as a Firewall.

A Firewall acts as a barrier to stop outside sources from gaining access to your computer by blocking unwanted network traffic. More simplistically, it will block network traffic from getting to your computer if your computer didn't initiate the conversation in the first place.

Internet Protocol (otherwise known as IP or TCP/IP) works by transmitting and receiving data on what are known as "ports". There are 65,535 ports available, and some have defined standards for a particular type of communication.

Common ports are:

| Port | Name | Common use |
|--------------|---|---|
| 80 | Hypertext Transport Protocol (HTTP) | Transmit/Receive web page content |
| 8080 | Secure Hypertext Transport Protocol (HTTPS) | Transmit/Receive encrypted web page content |
| 21 | File Transfer Protocol (FTP) | Transmit/Receive files |
| 25 | Simple Mail Transfer Protocol (SMTP) | Transmit email to a mail server |
| 443 | Secure Socket Layer (SSL) | Transmit/Receive encrypted data streams |
| 110 | Post Office Protocol 3 (POP3) | Retrieve email from a mail server |
| 119 | Net News Transfer Protocol (NNTP) | Public news groups commonly known as Usenet |
| 1433 1434 | Structured Query Language (SQL) | SIMS .net database / Veritas Backup Exec 9 or 10 / APC PowerChute Business Edition and many other database driven applications. |

Unfortunately, because certain ports allow incoming connections, they leave your system open to hackers if suitable controls are not put in place. If a port is allowing incoming connections it is known as "open", and if not it is known as "blocked" or "firewalled".

For example, if Microsoft Internet Information Server is installed on your computer (this is commonly installed on file servers, but not often on workstations), there is a good chance that many of the ports listed above are actually open.

In the case of file servers, these ports will normally be open to allow the file server to perform its role.

If you have Microsoft Exchange installed, port 25 is likely to be open so that it can receive email from the Internet.

In the case of workstations however, it is very unlikely that you will need many ports open.

Microsoft offers a built in Firewall with Windows XP Service Pack 2. If you have Service Pack 2 installed on your computer (click Start, Run and type WINVER to find out), consider enabling the firewall to block any open ports. If you don't have Service Pack 2 on your computer, why not! See the earlier section on Windows Update to find out how to get it.

If you are using an Operating System other than Windows XP, consider 3rd party firewall software. Network Associates McAfee Enterprise version 8 has a built in firewall. Symantec, Norton and many other well known software manufacturers offer more comprehensive firewall solutions.

Capita recommends

Install Windows XP Service Pack 2 and enable the Firewall. If your computer is hosting a SIMS database, the SQL ports identified above (or possibly different Ports depending on how your system is configured) will need to be opened.

For other Operating Systems, if you use McAfee Anti-Virus, consider updating to McAfee Enterprise version 8 which has a built in Firewall.

Firewalling external links

A dedicated Firewall can be installed on your network to filter any unwanted Internet traffic trying to reach your network. It should be the only physical connection between your network and any links to the Internet. In this way, all network traffic inbound to your site is passed through the Firewall. The Firewall examines and blocks data if it doesn't match a certain set of rules.

Firewalls are expensive and need specialists to set them up, but they give you increased security over any other method.

Capita recommends

Although most schools Internet links are firewalled by the LEA or Internet Service Provider and sit inside what is known as a "cloud", it won't necessarily stop other sites that are also within the cloud from being able to reach your network.

Enquire how well protected you are by talking to your service provider. If the level of protection is not as great as you would like, purchase your own Firewall.

System Resilience

What happens when your computer suffers from a hardware failure or power loss? These situations don't occur frequently, but do you know what action to take when they do?

Hardware Warranty

Computers are sold with some form warranty; the type of warranty will depend on the manufacturer. Purchasing from a major manufacturer such as Dell, HP or Compaq will usually give you three years On-Site Warranty. This can normally be extended at the point of purchase for an additional fee.

The recommended lifetime of a computer is three years, so this is the optimal period to get cover for.

When your computer suffers from a hardware fault such as a damaged hard disk or faulty CD-ROM, a call placed to the manufacture will generally result in the faulty component being replaced at no extra cost to yourself.

There are exceptions to this. If the component is physically damaged due to neglect, or is classed as a "consumable" part, you will have to bear the cost of replacement. Printers have many consumable parts in them such as the drum, fuser and rollers – always consider the running cost over the intended lifetime of use when purchasing printers.

Component parts purchased after the computer such as larger capacity tape backups or extra hard disks are not normally covered by On-Site Warranty and can be covered by Warranty or Return to Base Warranty, so enquire about this when expanding or upgrading computers.

Here is a general description of the different warranty types:

| Warranty type | Description |
|-------------------------|---|
| On-Site Warranty | The manufacturer will send an engineer to confirm the cause of the fault, and replace components as required to fix the physical problem. |
| Warranty | The end user is responsible for confirming the cause of the fault to the manufacturers' satisfaction. This normally involves running diagnostics and swapping alternate parts to prove the component itself is faulty. The part will then either be swapped by the manufacturer or must be shipped to back to the manufacturer for replacement or repair. |
| Return to Base Warranty | As with Warranty, but once confirmed, the component must be shipped back to the manufacturer for replacement or repair. |

Under the terms of Capita's Administration support contract, we will fault out hardware and liaise with the manufacturer for all warranty types to get the physical fault resolved. If you have a Partnership contract, due to the limited nature of on-site support we can only handle On-Site Warranty on your behalf. We will however assist as best we can with the other warranty types.

It is important to remember that replacing the faulty component is not always the end of the story. If the hard disk is replaced, there is a possibility that data may need to be restored from tape or another "mirror" hard disk. It is therefore wise to have good support for your systems.

Capita recommends

Purchase equipment from reputable manufacturers.

Investigate the cost of ownership before committing yourself as buying the cheapest normally incurs high running costs.

Enquire about the type of warranty you will receive on new purchases.

Maintenance

Once warranty has expired, you will have to bear the cost of any faulty components if you don't pay for hardware maintenance. If originally purchased through Capita, we will send you a hardware maintenance invitation near the time the warranty is due to expire.

If you receive a hardware maintenance invitation and don't take it up, future faults will incur charges for not only the components that are faulty, but also the cost of any re-installation required. In some cases it is actually more cost-effective to replace computers than fix them.

Maintenance is a form of insurance and as such cannot be backdated. Keep good records of when warranty will expire and either replace equipment or purchase hardware maintenance as necessary.

Capita recommends

Purchase hardware maintenance for equipment you plan to keep beyond its lifetime.

Consider replacing items that are about to go out of warranty in your capital expenditure plan.

Power

Uninterruptible Power Supplies (UPS)

Uninterruptible power supplies are designed to provide power to devices plugged into them when the utility supply fails.

UPS's are basically intelligent batteries. They detect if the utility supply is below a minimum voltage (brownout), or above a maximum voltage (spike or overvoltage) and boost or trim the power to 240V as required.

During a complete utility loss (blackout), a UPS will switch to battery, supplying 240V until the utility power is restored or the battery runs flat. The UPS can be configured to automatically shut down an attached computer cleanly. You can configure the shut down time to be a few minutes after a blackout, or a few minutes before the battery is about to go flat.

The power capacity of a UPS is measured in VA or Volt Amps. The higher the VA rating, the longer it will last. Standard UPS's are supplied between 350VA and 3000VA.

The length of time the UPS will be able to provide power will depend on the power consumption of the attached devices. An average fileserver running on a 1000VA UPS will probably keep running for around 40 minutes. Plug the same fileserver into a 3000VA UPS and it will probably run for 2 hours.

Once utility power is restored, the UPS will recharge, and can be configured to automatically switch on an attached computer.

Putting a UPS on your fileserver or standalone will keep your critical data from becoming corrupt during a power failure.

If you have a large network, consider putting a UPS on your network infrastructure (hubs, switches, routers etc) and key workstations. This then allows workstations running critical applications to be logged off cleanly before being switched off.

One word of caution though, UPS batteries don't last forever. Software supplied with most UPS's will perform periodic testing of the batteries and warn if they have failed. In this event, the UPS batteries can be changed, but it is often more cost effective to trade in the UPS for a new one. This avoids problems with battery disposal, and other complications that come with changing UPS batteries.

Capita recommends

Purchase a UPS for your fileserver or standalone. Configure it to automatically shut down your computer during an extended blackout.

Consider putting a UPS on devices that make up your network infrastructure.

Consider putting a UPS on key workstations running critical applications.

If your UPS batteries fail, trade in the UPS for a new one.

Redundant Power Supplies

Many fileserver and high specification workstations can be purchased with redundant power supplies. This simply means that two power supplies are fitted, and should either one fail, the computer will continue to run.

If you also have a UPS, you can provide three levels of fault tolerance by plugging one power supply into the mains and the other into the UPS. Then if the mains supply, the UPS or one of the power supplies fails, the computer will continue to operate normally.

Capita recommends

If purchasing a new fileserver, buy one with a redundant power supply.

Plug one of the redundant power supply cables into the mains, the other into a UPS.

Disk Space

It is important to ensure that your Standalone or Fileserver doesn't run out of disk space. Allowing this to happen will stop the computer working, and possibly lead to data corruption.

Any Fileserver running Windows Server 200x will most likely be configured with Active Directory. Active Directory is a database that holds the configuration of your network. If there is insufficient disk space to allow it to grow, your Fileserver will simply stop working, resulting in a lengthy and time consuming operation to repair it.

Any computer running SIMS .net will host a SQL database. As above, if there is insufficient disk space to allow it to grow, your SIMS data may become corrupt and or suffer data loss.

Capita recommends

Periodically check each drive letter on your Standalone or Fileserver (normally C: and D:) to ensure at least 10% of disk space is available.

Equipment Location

Think carefully about the location that equipment is sited. Electronic equipment will degrade more quickly if exposed to extreme temperatures and poor air quality.

Do not place equipment in direct sunlight; this will result in extreme fluctuations of the internal temperature, causing components to degrade more rapidly.

Wherever possible, avoid dusty locations. Dust builds up on internal components resulting in heat and static build-up, and in extreme cases electrical short circuit. If you work in a naturally dusty environment ensure it is cleaned regularly and vacuum any air vents on your equipment. You should also consider getting a suitably trained company or individual to periodically clean the internals.

Allow adequate airflow by leaving space around air vents. Don't place equipment close to walls or in confined spaces.

Fileservers should ideally be placed in a climate controlled environment. If air is too dry, an increase in static will result; this can in turn cause spurious crashes and errors. If air is too hot, components will overheat and simply shut down or age prematurely.

If you have a lot of Fileservers or network infrastructure, host it in a dedicated room with air conditioning. This will ensure the temperature and humidity is regulated, thus providing the optimum environment for computer equipment.

Capita recommends

Site equipment out of direct sunlight.

Ensure the environment is cleaned regularly and vacuum air vents.

Periodically clean the internals of computers in naturally dusty environments.

Consider a dedicated air conditioned room for Fileservers and network infrastructure.

SIMS .net SQL Database

Because SIMS .net stores all its data in one location – the SQL database – there are specific issues that you should be aware of to ensure the integrity of your SIMS system.

Backing up SQL

An SQL database cannot be backed up if the windows SQL service that hosts the database is running. As it is running all the time, you should either stop the service to get a backup, take manual backups from within SIMS System Manager, or purchase a SQL agent for your backup software.

The easiest option is to modify your overnight backup job to run a Pre-job batch file to stop the SQL service before the backup starts, and subsequently a Post-job batch file to restart the SQL service after it has finished. This is the only option for Standalone computers.

Capita can supply you with these batch files, and instructions on how to modify your backup job. These are available on request by contacting the Capita Education Service Desk on 01245 213911.

Stopping and starting the SQL service is less practical if you have other systems that talk to the SQL database overnight, if you have a Bromcom system for example. If this is the case, you either have to rely on taking manual backups from within SIMS System Manager, or to purchase a SQL Agent for your backup software.

Taking manual backups obviously relies on people – which lets face it, are not as reliable as we would like – which has inherent problems if staff are unavailable, forgetful or just too busy. Purchasing a SQL Agent for your backup software is an expensive option, but it will guarantee that you get a good backup no matter what happens.

Capita recommends

Purchase a SQL agent for your backup software. If you cannot afford this, modify your backup job to include pre-job and post-job batch files.

Take a manual backup from within SIMS System Manager once a month. Only keep a limited number of backups on the system as they use a large amount of disk space. If you have plenty of disk and tape capacity keep the last twelve backups, otherwise only keep six.

Database Size

SIMS is supplied with a free SQL database engine called MSDE or Microsoft SQL Desktop Engine. Many people are not aware that this has a database size limit of 2GB.

If you have a large school, enter lots of Attendance data or use Lesson Monitor, there is a good chance your SQL database is reaching the MSDE 2GB size limit. If the database reaches this limit, SIMS will simply stop working.

Capita has a utility available on our web site (www.capitadesktop.co.uk/home) that will examine your SQL database and advise you if it is 1.5GB or greater. If this is the case, we recommend you contact our Advice & Sales line on 01245 213913 and purchase Microsoft SQL Server Standard with an appropriate number of Client Access Licenses. Capita can supply and install this for you, thus ensuring your system doesn't suddenly stop working.

Capita recommends

Periodically check the size of your SQL database. If it approaches 1.5GB in size, plan to migrate from MSDE to Microsoft SQL Server as soon as possible.

