
Focus on your business – Not your technology



Business Technology Guide
Technology Management – In Plain Language

Table of Contents

TECHNOLOGY LIFECYCLE MANAGEMENT	1
STAGE 1 – ASSESS AND IDENTIFY	3
CHOOSING THE RIGHT COMPUTER FOR A BUSINESS	6
DIFFERENCE BETWEEN A SERVER AND DESKTOP	13
LOW COST TECHNOLOGY	17
CLOUD COMPUTING.....	19
GREEN TECHNOLOGY.....	21
STAGE 2 – TECHNOLOGY ACQUISITION	23
LEASE OR HIRE TECHNOLOGY	24
CONNECTING OFFICES	26
STAGE 3 – INTEGRATE AND IMPLEMENT	28
ELECTRONIC DOCUMENT STORAGE	29
PROTECTING YOUR DATA FROM UNAUTHORISED ACCESS.....	31
CONNECTING TO YOUR BUSINESS WHILST TRAVELLING	33
TECHNOLOGY SECURITY TRAINING	35
SECURITY POLICY	37
E-MAIL POLICY	39
ELECTRONIC DOCUMENTS AND THE LAW	41
DISASTER RECOVERY AND BUSINESS CONTINUITY MANAGEMENT.....	43
STAGE 4 – SUPPORT SERVICES	46
SUPPORT OPTIONS.....	47
STAGE 5 – TECHNOLOGY REFRESH	48
STAGE 6 – ASSET DISPOSAL.....	49
RECYCLE OLD TECHNOLOGY	50

Technology Lifecycle Management

Overview

Underpinning the majority of business is technology which requires management encompassing more than a simple “lights on” philosophy. Technology management in a digitally driven economy is much more than just buying a computer from the nearest electrical store.

Your technology infrastructure may be the single most important production asset you have - in terms both of maintaining business continuity and delivering the kind of performance that will keep your business competitive.

So, ensuring that your technology functions optimally is most likely a key strategic objective for your business.

However, the majority of technology infrastructure, including your own, is at risk from security vulnerabilities, configuration drift, end of life issues, licensing compliance and will remain so through upgrades and the addition of new technologies unless the infrastructure as a whole and its individual assets are properly understood and holistically managed.

Therefore Not-a-Geek recommends a Technology Lifecycle Management (TLM) approach that will help ensure your technology assets continue to support your business over their lifecycle, from “cradle to grave”.

TLM is a philosophy for enabling systematic budgeting and administration of technology infrastructure. It addresses the challenges posed by technology management and provides the most functional, flexible technology infrastructure possible, at the lowest cost of ownership

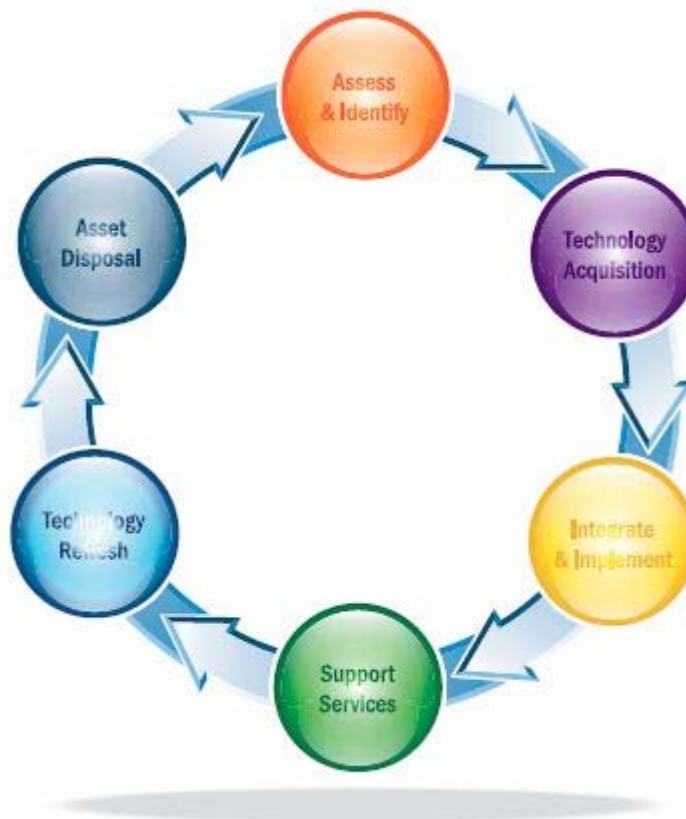
Here at Not-a-Geek we have adopted business practices from over twenty years experience in managing technology and built it back into a range of solutions and services that eliminate waste, risk, and uncertainty from your technology infrastructure investment.

For the small to medium business such an approach may seem complicated and expensive. This does not have to be the case and the purpose of this guide is to provide some thoughts on the key strategic technology decisions and how best to build your own TLM strategy.

- **Assess and Identify**—this process addresses every phase of the technology lifecycle so that future business needs, technology requirements, financial considerations, and expansion plans are anticipated and addressed from the start. This involves developing logistics, deployment timelines, technology health check schedules, refresh cycles, and asset disposal plans. It provides a long-range view that anticipates and addresses next-generation technologies that should protect the technology infrastructure from obsolescence due to unexpected budget shortfalls or the inability to scale to meet expansion requirements.
- **Technology Acquisition**—this process includes procurement, logistics planning and finalisation of financing. To simplify this stage, many businesses outsource some, if not all, acquisition-related tasks. A common practice is to have a technology solution

provider project manage the acquisition, deployment, and implementation of the technology.

- **Integrate and Implement** - this process covers the integration and implementation of the infrastructure solution mitigating risks, and maximising efficiencies and asset tracking. This is important for ensuring technology security and the businesses ability to recover vital assets and information. Such asset tracking has become more difficult in recent years due to increases in worker mobility and the prevalence among businesses to take a siloed approach to adding technology assets.
- **Support Services**—the importance of post-implementation support services that enable high infrastructure productivity are critical to a successful business. These services, such as on-going proactive maintenance keep the technology infrastructure operating in its optimal state at all times.
- **Technology Refresh**—under a traditional capital acquisition plan, funds that were allocated for refresh may go to other projects within the business through a lack of strategic planning. With TLM, the funds for refresh are secured since a strategic plan is documented being followed by the business. This enables the upgrade of technology infrastructure to keep up with increasing user demands and applications and prevent system failures and service interruptions.
- **Asset Disposal**— some businesses may choose to cascade technology to administrative or other business units that do not require the most advanced technology. The business should assess the true cost of re-purposed technology such as security risks, patches and replacement parts, and out-of-warranty repairs.



Stage 1 – Assess and Identify

The first stage in TLM is to assess the business and technology objectives and identify end-user needs.

A key element of this process is to address every phase of the technology lifecycle so that future business needs, technology requirements, financial considerations, and expansion plans are anticipated and addressed from the start. This involves developing logistics, deployment timelines, technology health check schedules, refresh cycles, and asset disposal plans. It is a long-range view that anticipates and addresses next-generation technologies that should protect the technology infrastructure from obsolescence due to unexpected budget shortfalls or the inability to scale to meet expansion requirements.

The results of the business requirements analysis and technical environment evaluation specialists are evaluated and documented in both short-and long-term recommendations. This report also should include;

- An acquisition strategy
- Financial plans aligned with budget availability
- A plan for ongoing support
- A project implementation plan
- An asset tracking and retirement strategy

Completing this phase requires several high level initiatives.

Business Objectives and Needs Analysis

The assessment of a business's objectives and the identification of the business processes form the framework for the recommended technology architecture. This serves as a working model for the development of a technology infrastructure that continually supports the underlying business processes and objectives.

Technical Environment Evaluation

It is vital that the business select a procurement vendor that understands the business processes supported by the technology infrastructure. A technical evaluation specialist identifies the best technology architecture for each environment. The results drive the requirements for the technology components and services to be integrated into the existing infrastructure. Consequently, the business can right-size the technology architecture for flexibility to meet current and future user demands, performance requirements, and applications.

Through close examination of existing customer resources and the legacy systems comprising the current infrastructure, an evaluation of the technology that will meet forecasted capacity and enhancement requirements over a span of years can be undertaken. Analysing the lifecycle of the technology, correlating quantifiable costs and benefits to each lifecycle stage, and providing financing options can accelerate deployment of the technology infrastructure.



Technology Selection and Acquisition Strategy

Specifications for the appropriate technology are created from the results of the technical evaluation and needs analysis. The end-user needs analysis, which involves identifying and categorising specific business, operational, and technical needs. Defining requirements and expectations from the customer/ user perspective, provides the details for an outcome plan. When developing this plan, consideration must be given to factors such as customer resources, legacy systems, forecasted capacity, laws and regulations, and anticipated areas of enhancement.

A strategy for vendor selection is developed based on a review of “Commercial-off-the-Shelf” (COTS) products and a determination of how each product can satisfy criteria for innovation, longevity, and viability as they relate to the business objectives.

Technology Validation and Refresh Cycles

Regularly scheduled reviews and assessments of the technology infrastructure enable business to ensure that the technology integrated into their technology infrastructures continues to perform to expectations.

When it becomes evident that the currently installed technology no longer has the capacity or capability to support the business need, components can be swapped for new or updated technology.

Effective financial planning and management make appropriate technology refreshes easier by proactively developing a replacement strategy for assets prior to initial deployment. This approach enables consistent budgeting, offers the flexibility to respond to change, and promotes continuous performance improvements.

Spreading acquisition costs over the life of the asset protects the business from experiencing both spikes and shortfalls in their capital budgets.

Logistics Planning and Deployment Scheduling

Once the business has determined its refresh cycle, a deployment schedule can be developed based on an analysis of the age and capabilities of the technology integrated into the existing infrastructure. Depending on the state of the current computing devices, the size of the business, and budgetary cycles, the deployment may need to occur all at once or be phased in over time. Phased trade-in programs are useful in streamlining the implementation and integration processes by cycling older technology out of the business as part of the new technology acquisition plan.

Asset Disposal Strategy

A complete assessment of the costs and resources required to manage assets through the entire technology lifecycle enables the business to plan for the disposal of the devices when they reach the end of their useful life. Asset disposal factors to consider include potential resale value, disposal costs, and services required to securely uninstall data and remove equipment. Although predicting resale values and asset disposal costs is not typically a core

skill of the businesses, it is a critical element in managing the costs of the technology infrastructure.

Costs for contracting with environmental specialists must be factored in if outside services are needed to comply with environmental and security regulations. Regardless of the method of disposal (donation, resale, or destruction), there are additional costs associated with the destruction of data stored on the equipment, which may require degaussing the hard drives or using commercially available erasure tools.

Financial Planning

Technology acquisitions historically involve large appropriation requests and capital expenditures.

Because the benefits of investing in technology are often derived over time, it is difficult to capture Return on Investment (ROI) incrementally. At the same time, the long budget cycles inherent in capital appropriations create an understandable bias toward owning technology assets, as businesses attempt to mitigate future budget cuts that could prevent them from procuring needed equipment. Under this scenario, the entire budget justification, appropriation, and procurement must be repeated for each technology refresh, upgrade, and addition to the infrastructure.

A paradigm shift has made it increasingly common for the business to classify their technology infrastructures as an operating expense rather than a capital investment. With pay-for-use programs and financing, businesses can manage and expense their IT infrastructure as a service.

A proactive financial strategy supports the technology lifecycle by;

- Recognising the need for flexibility to acquire new technology, refreshes, and upgrades
- Responding to the limited useful life of technology assets
- Developing a pay-for-use program and outsourcing the responsibility of ownership, implementation and maintenance services, and asset disposal
- Expediting the delivery of business objectives through technology
- Addressing IT as a service

Once the technology and implementation resources are identified, a refresh cycle determined, and a disposal strategy developed, the business has a good picture of the financial resources required to implement. The funding of pay-for-use programs using operations and maintenance budgets treats the use of technology as a service. In this view, ownership is not a requirement, and is often not preferred. This utility approach has become a recognised best practice and supports the trend toward performance-based contracting.

Choosing the Right Computer for a Business

Introduction

Whatever the type of business, it's rare to find one that doesn't have a computer at its heart. Able to manage everything from accounts to stock control and customer communications, a company computer is a critical purchase which should be chosen keeping the specific needs of the business in mind.

But for even the most technologically-minded of business owners, selecting the right computer from the vast array of manufacturers and models can be a daunting task. With a market that's crowded with desktop computers, laptops, PDAs, notebooks and the latest tablet computers – operating on varying operating systems, identifying what the computer is actually for is a critical first step.

Factors to consider include;

- How will the computer be used?
- Does the computer need to be mobile?
- How much processing power will the computer need?
- Will the computer need to connect to peripheral equipment and other computers?

Once these questions have been answered, deciding which type of computer is right for the business becomes a little more straightforward.

Key Considerations for Computer Purchase

- **Assess business needs**—what will the computer be for? Which applications will it need to run and what are the objectives for purchase?
- **Consider the user/s**—who will be the primary user of the computer? Do they have any particular needs or requirements for the computer and how it operates?
- **Support and warranty**—is the support and warranty sufficient for the needs of the business? Would extended cover offer peace of mind/ good value for money? Is there a contingency plan in place should the computer fail?
- **Mobile or desktop?**—does the computer need to be mobile? Will it be used extensively in an external environment? Are there any restrictions in terms of space, power and networking capabilities?
- **Hardware and software**—which applications will be run on the computer? Will the computer be running any memory-intensive programmes? Is additional RAM or processing speed required?
- **Operating systems**—is the operating system installed sufficient for the business's needs? Is an upgrade worth an additional outlay? Does the computer come with operating system disks or are they easy to access in case of a system crash or virus?
- **Buy or lease?**—the tax and accounting advantages of any new computer purchase should be closely assessed. The timing of purchases and use of finance can also have a significant impact on the overall cost of computer equipment. Does leasing equipment provide a more cost-efficient option?



Technical Support

Adequate support and warranty cover for a business computer is essential. Some retailers will offer a complete replacement service for a computer that fails. Others will only offer telephone technical support in the first instance, with a back-to-base or on-site repair service only in extreme circumstances. If the computer has to go away for repair, what alternatives exist for technology whilst this device is away? What confidential data may be stored on the hard drive?

It is critical to check the small print. Usually an extended warranty can be arranged for an additional fee, and this can be well worth it if it means a business can continue to operate.

It's important to consider the details of this agreement carefully – policies and costs can vary greatly, but it is vitally important to ensure computers can be repaired or replaced if they do fail.

Desktop Computers

Traditional Design

For a business with a traditional office and staff that don't need technology on the move, a desktop computer can be an ideal choice. Businesses can choose from a range of computer designs from slimline to workstation, "white box" or brand name, a broad range of processors and more memory and storage to manage all of the company's information within a single unit.

Thin Clients

Businesses looking to minimise desktop support costs may wish to consider 'thin client' computers, which are smaller than standard computers. Thin clients have little on-board memory or external connectivity, but are ideal for businesses that want to connect several computers to a central server to operate on the network. By reducing the memory and processing power of individual computers, cost and office space is saved, yet operation is efficient as these requirements are met by a more powerful server.

Advantages of desktop computers;

- Low purchase price
- Easy to upgrade
- Many peripherals available
- Large screen sizes
- Comfortable to use for long periods

Disadvantages of desktop computers;

- Bulkier than other options
- Require a separate monitor and keyboard
- Only suitable for traditional office-based operation

Mobile computers

Laptops have changed dramatically over recent years – evolving from heavy, underpowered devices to lightweight computers that match the processing powers of a desktop computer. From the smallest of notebook computers to heavy-duty laptops designed to cope with the rougher treatment of life outside of an office, the capabilities of mobile computers are incredibly wide-ranging.

Laptops and notebooks

Giving businesses a balance of portability and office performance, desktop replacement laptops deliver the memory and connectivity to match a desktop computer. The slightly smaller notebook computer offers mobile businesses an exceptional level of on-the-go and office-based business performance, but often lacks the connectivity of larger counterparts.

Net Books

At the smallest end of the scale there are net books, which are basically small notebook computers. These offer limited processing power but are great for accessing e-mail or appointment lists on the move, or viewing websites. These are not suitable for intensive applications such as working on spreadsheets.

Tablets

The latest addition to the mobile computing market is the tablet computer. These touch-screen operated computers are, in essence, notebook computers without a physical keyboard and offer high-levels of out of office functionality.

Advantages of mobile computers;

- Lightweight and easily transported
- Can have just as much processing power as desktop computers
- Allow wireless access to the internet when working remotely
- Consume less energy

Disadvantages of mobile computers;

- Smaller screen sizes
- Reduced multimedia capabilities
- Difficult to upgrade some components
- Generally more expensive than desktop computers
- Higher risk of a governance issue through loss or theft

Comparing the Costs

Buying a business computer can mean an investment of anything from a couple of hundred to several thousand dollars. A popular choice for small businesses is the office based tower system computer. Starting at around \$700, tower systems offer simple memory and hard drive upgrades as and when they're required, making them a cost-effective choice for a developing business.

Desktop computers bought directly from a retailer will often have a basic mouse, screen and keyboard included. However, computers purchased online or direct from the manufacturer tend to be built to order, which usually gives the option to select peripherals individually. This can be preferable, since there is a vast selection which can be specifically chosen to suit a business's budget and requirements. For example, ergonomic keyboards and large screens are ideal for heavily-used computers, whilst wireless mice and keyboards offer more desk flexibility as they can be moved easily to create more work space.

Many businesses find the flexibility of a laptop appealing and are often willing to pay a slightly higher price tag for the processing power and features of a desktop with the added benefit of portability.

For businesses that have a need for extensive processing power, a move into the specialist sector of workstations is worth consideration. Additional memory, faster processors and improved graphics make these computers a good solution for businesses using their computer heavily and relying on high levels of performance. These are not for the budget end of the market however, with prices ranging from \$1500 for an entry-level workstation to over \$3000 for models able to deliver highly specified graphics.

Processor

For most businesses, a processing speed of around 2.5 Giga Hertz (GHz) is ideal for desktop computers, 2GHz for laptops. This gives the computer enough raw processing power to handle office tasks, internet access and applications such as Microsoft Office.

As a rule, the faster the processor, the quicker and more efficiently the computer will run. However, for businesses not manipulating large amounts of data or using graphics programmes, specifying a very fast processor is usually a false economy, as the speed will not be used and it would be more beneficial to divert any funds to other specifications like extra memory.

Memory and hard drive

Alongside the processor, the memory and hard drive are crucial components to consider when choosing a business computer. The higher the RAM (Random Access Memory), the more efficiently the computer's operating system will run, and the minimum recommended level for a business computer is 4 Gigabytes (GB). If additional RAM is required it is usually most cost-effective to request this as the computer is ordered as the configuration and types of memory can vary widely.

Due to their design, it is more complex to add RAM or hard disk memory to a laptop computer, so it is important to ensure these levels are adequate at the time of ordering. The minimum levels recommended are similar to those for desktop computers.

Unlike with RAM, the size of a computer's hard drive is not the prime consideration;

- **Type** - a hard drive can contain moving parts, which if then installed in a mobile device which is handled roughly could lead to damage. For such scenarios consider a solid state drive, although these are considerably smaller in capacity and more expensive.

- **Speed** - if the disk has moving parts the faster the revolutions the better, with common metrics being 5400 rpm, 7200 rpm, 10000 rpm and 15000 rpm.
- **Controller** - the type of controller will also affect the speed of the disk with options generally from SATA and SAS. Either type can have different versions which will affect speed, for example SATA-1 1500Mbps compared to SATA-3 v3 is 6000Mbps.
- **Size** - on one hand the bigger the better, but then you have to consider the more data you are backing up the higher the risk of data loss from a single device, which may affect your backup decisions.

A general recommended size of 320GB should be more than sufficient. This gives enough space for all required applications to be installed and enables the operating system to run efficiently.

Monitor and Connectivity

Monitor

However efficiently a computer operates, if the screen is unclear or too small it will always be difficult to work with. Standard business monitors start at 17-inches with a resolution of 1280 × 1024 pixels, and this is usually more than adequate for general office use. Depending on the type of business and the way in which the computer will be used, a larger screen or a higher resolution may be desirable.

Larger screens have been shown to allow employees to work more efficiently, and with the difference in price between a 17-inch monitor and a 20-inch monitor as little as \$300, it can be preferable to choose the larger option.

The monitor is driven by a graphics card, and standard versions are usually shipped with the computer. Standard graphics cards can sometimes share the computers main memory, whereas others will have their own dedicated memory. If a very large monitor is being used, or the computer is used for highly specialised tasks such as graphics work, more consideration into the specification of graphics card will be required, the more intensive the graphics work the more dedicated graphics memory will be required.

As laptop screens are part of the computer themselves, they cannot be upgraded as a desktop monitor can. Most business laptops will have a screen between 15.5 and 17 inches, and the decision on the size of the screen can often be made by considering the trade-off between usability and portability.

For the best of both worlds, a larger monitor can be attached to the laptop when it is being used in an office. This can be either directly or via a docking station – a port to which the screen (and other peripherals, such as a printer and mouse) can be permanently attached, ready for the laptop to be connected.

Connectivity

Desktop and mobile computers usually include a selection of standard ports for peripheral connection. USB ports connect printers, keyboards, memory sticks and a whole host of other peripherals, whilst an Ethernet socket enables connection to a network router for internet

access. Internet access will require the computer to have a network card. This is usually built in, but if not, can be purchased and installed cheaply and simply on desktop computers.

Wireless networks are used increasingly within and outside the office environment. Connecting to these requires a computer to have wireless network capability; this is commonly built-in as standard on laptops but may require additional hardware to be installed on a desktop computer. However consider the security risks of wireless, by virtue of the technology having no boundaries; a poorly configured wireless network could be an easy target for a hacker outside the business perimeter.

Care should be taken when selecting a connectivity medium since the speeds with which data can be transferred across them do vary. For example, external USB disks are easy to use and often come in large capacities but they may not be suitable for enterprise backups since USB is relatively slow compared to other connectivity mediums.

Operating Systems

An operating system is mandatory software that controls the basic functioning of a computer. By far the most popular is one of the versions of Windows available from Microsoft. Alternatives include Mac OS X and Linux.

All operating systems have a supported life and this should be factored into the plan. For example many businesses still run Windows XP, they see no reason to upgrade, and the operating system performs the functions they require. However Microsoft stopped supporting this version in April 2009, which may now present a security risk to the business that has to be managed.

Most new computers which have the latest Windows 7 operating system installed will have the Home Premium edition. An alternative to this is Windows 7 Professional, which can usually be selected as an upgrade option if business needs dictate.

It is recommended that a business does not purchase the Home Premium version choosing instead to use Professional version. This version also features a mode where Windows XP applications can be run within the Windows 7 Professional environment – enabling legacy applications requiring Windows XP to continue to function. Windows Professional is available in 32 or 64 bit, with the former more than suitable for the majority of business purposes. If you select the 64 bit version some care must be taken to ensure that and peripheral drivers and additional applications are compatible.

Many operating systems come pre-installed, but it's crucial to obtain, or have access to, a copy of the operating system on a disk should a serious system crash or virus affect the computer. This will allow the operating system to be re-loaded and the computer to be back in action as quickly as possible should the worst happen. If a new computer does not come with media it can usually be created when the machine is first switched on.

Apple Macintosh computers are not generally seen in a business environment, they are usually associated with media intensive industries. If considering an Apple computer make sure the vendor support options are reviewed carefully, you may find it difficult to locate a support person other than the store you purchased the computer from.

Where to Buy

Business computers can be bought directly from the high street or online. It's possible to either buy from an online retailer, a value add reseller or direct from the manufacturer – and in both cases peripherals can usually be ordered at the same time. The key thing to consider when selecting the vendor is the after sales support—will they assist the business with post sales or leave the responsibility to the business?

Green Disposal

Disposal of computers and related equipment is an important consideration for any business. It is estimated that there are 315 million redundant computers in the world. Of these, around 50 per cent will be discarded and disposed of in landfill sites. In an attempt to reduce this environmental burden and promote the responsible disposal of waste electrical equipment, in Europe the Waste Electrical and Electronic Equipment Directive (WEEE) has been developed. Whilst this scheme is not enforceable in Australia, it would be a good example to set. If your disposing of technology check with your local council for “electronic waste” facilities rather than just dumping in land fill.

In essence the Directive compels all businesses to conscientiously dispose of all their redundant or obsolete electrical equipment in a responsible manner. The Directive not only covers the correct disposal of desktop and laptop computers, but also a keyboard, mouse and other peripherals.

How can Not-a-Geek assist?

We offer a holistic assessment scan of the technology currently deployed in your business. From this information we can map out the technology landscape identifying strategic key areas for review.

Our assessment is non-intrusive and respects the data confidentiality of your business. The information gathering can be completed in a couple of hours and the report prepared two to three days later.

Difference between a Server and Desktop

Introduction

A large proportion of small-to-medium business uses an old desktop computer as a “server”. This approach is fraught with risks. Whilst it will provide a central computer for the storage of data, a desktop computer is not designed with reliability and scalability in mind, which are two of the key criteria of a server.

Since more than one person will be trying to access a server at any one time, the reliability and scalability of server are very important and therefore a server should contain redundant parts, so no one part failure will jeopardise the operation of the server.

Do I Need A Server?

Most business people are familiar with desktop computers and understand some of the basic principles of what a computer can do. A server is similar to a normal desktop computer but generally is designed for greater reliability with redundant components to mitigate business disruption from component failure.

The server acts as a central repository of business data and is generally used to securely store electronic files and provide authentication to a number of networked computers.

Servers can also offer specialised application services like e-mail and database functionality.

Why Should I Bother With A Server?

Many small businesses can easily store all of the files they need on a single computer. If you work alone with a small amount of data this is a perfectly valid route to take, and a server would be of little benefit.

When you start to work with other people the chances are that you will want to share documents and files. If these are stored on one person’s computer then it makes it difficult to access the data in a multi user environment.

If you are using a large amount of data – possibly CAD/CAM drawings, video files, images or databases, it makes sense to store these files on a server that is optimised for handling large amounts of data.

By using a server your data should be more secure, more accessible and quicker to access.

How Much Will A Server Cost?

Prices of computer hardware vary enormously and it pays to explore the latest offers that suppliers may have running at any moment in time. Typically you can expect to pay these prices dependent upon the type of server you are after;

- **Budget server**—a no-frills computer with limited or no expansion capability and limited ability to protect your data in the event of a problem. It will support up to, say, 6 typical users, a typical price may be in the range of \$1000-\$1500.



- **Mid-sized server**—that has scope for expansion and which can continue to run after most kinds of component failure or problem. It will support up to, say, 20 typical users. A typical price may be in the range of \$2000-\$5000.

In practice there is a spectrum of servers in between and larger businesses can expect to spend considerably more for specialised specifications. You will no doubt find that the cost will rise when you come to configure a useful machine as the advertised headline price rarely includes operating or application software. It will certainly not include application software, installation or support.

What Features To Look For In A Server?

If you want to run a business application on the server as well, you should seek advice from the application developer or provider because business applications can have a major impact on performance.

Here are the typical features you will need to understand when purchasing a server.

Processors

A processor is the “brain” of the server. The better the processor then the more capable your server will work for you.

A budget server will use a single processor without any option to add a second.

A mid-sized server will have two or more processors (sometimes with two or more cores per processor) with the ability to run on just one if one of the processors fails. The ability to add further processors would be useful but, in practice, companies rarely upgrade processors after a server is installed.

More cores does not necessarily mean a better server since the operating system and application that runs on the server must be optimised in a such a way – multi threading – to take advantage of the extra cores.

Main Memory

Memory is the thinking and general work space for the server. The more memory, the more room to think and the faster the server will perform.

A budget server will come with 2GB of main memory, although 4 GB would give a significant performance boost for most applications.

A mid-sized server will have a minimum of 4 GB of main memory. Look for the ability to expand to at least 8 GB.

Some operating systems will only use a certain amount of memory even if more is added, so it pays to check the technical design limits of the software before investing.

When checking expansion capabilities verify how much main memory can be added to the supplied configuration. Main memory is fitted into slots and the way it is configured in a

supplied computer might mean the replacement of the original memory when you wish to upgrade leading to greater costs than expected.

Disk Drives

These are used to store your data. The bigger the disk drive, the more you can store on your server. Most small businesses will be fine with between 80 GB and 150 GB.

You should expect the server to support at least six drives, preferably more. It should also support several options that allow the server to continue without interruption even if one of the disk drives fails.

As minimum disks should be installed to act as a redundant pair (RAID 1) however other combinations of redundancy (RAID 5, RAID 10 etc) are available depending upon the role of the server.

Removable Media

You will need a CD/DVD drive in order to install software on the server. A writeable drive can be used for backup purposes. For a mid-sized server, you should consider adding a tape backup unit and supporting software.

Care should be taken when selecting a tape solution, specifically if considering a Disaster Recovery / Business Continuity plan. For example, it is all well and good having data on a tape but how do you read that tape at another location if the main tape drive is lost through a building fire.

Power

A budget server is more likely to fail if there is a failure in the power supply or a power interruption.

A mid-sized server will come with options for redundant power in the event of a supply problem. You will need to consider how vulnerable you may be to power problems and configure your server appropriately.

Since the server is generally the central computer in a network it should also be protected by an uninterruptible power supply (UPS), which will shut the server down in a graceful fashion after a certain amount of time has lapsed with no mains power thereby reducing the risk of data loss. However a UPS generally only protects the server – if you work on very sensitive documents then consider small UPS units for desktops also.

Operating Software

This is likely to be a significant part of the overall cost of the server. Make sure it is included in the price you pay or that you budget for it as an extra. If you intend to run business software on the server, check what licensing you need with the developer or supplier. Typical software on a server would be a product bundle designed for a small business. Other server software, although designed for home/consumer use, may be useful for a small business and be a bit cheaper. You may also need to consider other software such as e-mail products like Microsoft Exchange or Lotus Notes.

When purchasing software be careful you understand the licence restrictions. An entry level server operating system will allow for five client access licences (CAL), if you have more than five people connecting to the server you will need more CALs.

Server Support

On-site support should be considered mandatory for servers – the last thing you want in a business is sending your server away to a repair centre if a component fails. Failures should be rare, but you will be without a potentially key item of equipment while you are waiting for the server to be repaired. Think about whether you need cover outside normal hours.

Low Cost Technology

Low Cost IT Equipment

Naturally anyone in business will look for ways in which they can reduce costs, and so it is with the buying of computer hardware. Over the past few years the cost of IT equipment has fallen dramatically as the performance and functionality has risen due to improved production methods, technology and competition.

It is now possible to purchase a brand new laptop for around \$300. Are these real bargains or are they too good to be true?

Ultra low cost computers are a fairly recent innovation and have come about due to aggressive cost cutting and outsourcing of the production cycle. By ultra low cost we mean prices often 50 – 75% less than a mainstream branded computer. Recent innovations have seen not just desktop computers being sold at low prices but new laptops at around \$300, cheaper than many second hand branded laptops. One reason for this reduction in prices is an initiative by the computer industry to provide cheap laptop computers to people in developing countries. By definition these need to be built for a very low price but also provide acceptable performance and reliability.

Benefits of Low Cost Computers

The low price enables those businesses that would not have considered laptop computers to now purchase them for staff - probably “road warriors” or sales teams who travel out and about and need a basic computer. By having access to a laptop, mobile workers can work when they are out and about rather than wait until they return to the office – a real advantage.

It is also generally safer to purchase a new rather than second hand laptop. With new you would normally get a warranty so that if something goes wrong you are protected. Generally laptops have a tough time so a second hand one may have a relatively shortened life span. Fragile components such as the hard disk drive are always susceptible to damage. Second hand computers may also have data resident on the hard drive from the previous owner, even if they believe they have removed or erased it.

Downside of Low Cost Computers

Unfortunately there are some downsides to buying very low cost computers. The most obvious would be found when you switch the computer on. Instead of a probably familiar Microsoft Windows operating system you will most likely see a version of Linux, an open source operating system. Although this may be made to look somewhat like Microsoft Windows it is still different and you will need to learn new commands and controls. For some people this can be a major barrier to purchasing a low cost computer.

Some low cost computers can have Microsoft Windows XP installed, but this may have problems running to its full capabilities. Often in ultra cheap laptops the amount of memory available for the computer to use is limited. With an operating system such as Windows XP



loaded you will get slow performance and become very frustrated very quickly. It would not be possible to do anything on the computer other than real basics – certainly no image editing or graphics programs.

You may find the keyboard too small, but this is often the case even on more expensive lightweight laptops. You will probably find the screen is much smaller than you would expect as some ultra low cost laptops may only have a 7-inch low resolution display. This means that you may not be able to see much detail on the screen.

In terms of business data the reliability of cheap laptops needs to be considered. You would expect the hard disk reliability of a branded computer to be significantly better than that of an ultra low cost laptop, so the chances of data loss could be higher if you buy cheaper. This can be managed if you adopt good data backup procedures.

In summary pros and cons of low cost laptops are;

Pros

- Cheap
- Often more reliable than second hand
- Often more presentable than second hand
- Provides a good level of basic computer functionality

Cons

- Probably less reliable than a brand named
- Small screen
- Uses non-Windows operating system
- Relatively poor performance
- No advanced functionality
- Business data may be at more risk

Cloud Computing

Introduction

Many businesses own and manage their own technology, but often struggle to keep their systems safe and sound against a barrage of viruses and new software installations. They may also need to keep large amounts of customer or supplier data on server computers based in their offices. This computer management problem is especially bad if you have no interest in technology, and often results in expensive visits from technology support vendors. In addition you need to make room for your computers and keep them fully backed up and secure, plus pay for the electricity that keeps them running.



Cloud computing has evolved in an effort to address these issues.

Cloud computing uses the internet to connect your local computers with computers located many miles away (often in different countries) that run your key business applications and store your important data. You still need to be able to access the internet, so cloud computing does not remove the need for all your technology, but it can prevent you from having to run larger server based computers in your office.

Cloud computing is also referred to as Software as a Service (SaaS) or hosted software solutions.

There are three generic “types” cloud;

- **Private** – technology capabilities are provided “as a service” over an intranet, within the business and behind the business firewall
- **Public** – technology activities and functions are provided “as a service” over the internet
- **Hybrid** – internal and external service delivery methods are integrated

Benefits of Cloud Computing For Small to Medium Businesses

The great thing about cloud computing is that your data and systems are resident away from your offices. They are maintained by experts who are responsible for backing up and protecting your data. If you have a fire, flood or other disaster in your office you know that your essential data is safe and sound in this secured, remote facility. The company that looks after or ‘hosts’ your data will also be responsible for making sure anti-virus software is up to date and all the computers have their software patched.

Cloud computing is also useful if you are a new business and are unsure how your technology requirements may grow. With a cloud computing based solution you can simply ask your hosting company to add additional computers to your network according to your timescales and growth plans. Likewise they can turn off computers if business is a bit quieter to save you money.

Hosted applications can also benefit businesses as they can be accessed from anywhere in the world as long as you can obtain a connection to the internet. This is useful if you have a distributed workforce, maybe working from home.



Issues of Cloud Computing For Small to Medium Businesses

Of course there are some drawbacks to cloud computing solutions.

Data being held away from your site can be a disadvantage and in some instances you may not feel comfortable with your confidential data being sent across the internet and stored in another country. Indeed there may be legal issues with storing data remotely in some overseas countries. Other people feel that cloud computing takes away control of their systems and don't like having to ask a third party to make changes to a system configuration which can take time – often up to 24 hours.

It is not unknown, but fortunately quite rare, for a cloud computing service provider to have significant technical problems and prevent thousands of customers accessing their data.

A recent case in Australia saw a cloud provider become compromised which caused months of data to be lost from its customers systems. The end result being the provider was forced into liquidation.

These cases are readily publicised and cause huge embarrassment to the service provider so they are geared up to ensure it only happens infrequently. However “caveat emptor” should be a ready catch cry and the business should have a sound risk mitigation strategy and a proven business continuity plan.

Applications in a Cloud Computing Environment

Applications that generally work well by being hosted in a cloud computing environment include;

- Customer Relationship Management (CRM) systems
- E-mail
- Order processing systems
- Shared applications for collaborative working
- Data backups

Applications that generally don't work well by being hosted in a cloud computing environment include;

- Bespoke solutions created for your business that don't use internet technologies
- Applications that use a lot of graphics, rich media and video
- Office applications (such as Word and Excel)
- Applications that use confidential data

How can Not-a-Geek assist?

Leveraging our strategic relationships with IBM and VMWare we can provide the end-to-end cloud solution to satisfy the most demanding needs of any business.

Green Technology

Introduction

Few business people could fail to realise the importance of green or environmental issues that now affect all parts of our day to day lives. All businesses, no matter what size, can help to save resources. In addition, by reducing waste a business can save money and establish itself as a socially responsible employer.

Technology can contribute a fair amount to your running costs as well as your overall environmental footprint. Over the next few years legislation will increasingly start to affect smaller businesses and will start to force behavioural changes along with overall attitudes to the environment.

The good news is that we can start the process now, and by saving the environment we are able to save our businesses money. By supporting environmentally friendly technology initiatives today, you can be ahead of the game.

What Is A Green Business?

There are many measures of how green or environmentally friendly a business is, ranging from carbon footprints through to complex companywide audits. In practice it only takes a few steps to achieve considerable environmental savings and these need not impact upon the effectiveness of the business.

Generally the focus of the technology management is, of course technology. To that end it is advantageous to take a more detailed look at technology savings, but don't forget the non-technology related changes that can also help you become environmentally friendly. Remember, a green business is one that takes efforts to reduce its environmental impact overall and aims to become a socially responsible citizen.

Technology and the Environment

If you take a look around your workplace you are bound to have any number of computers and other technology in use. Technology takes resources and energy to create, run and dispose of and therefore each piece of hardware you use carries an impact on the environment. There is little we can do to influence the creation of technology equipment but there are things we can do that affect the day to day use of technology and its eventual disposal.

Computer Power Consumption

Of course computer equipment consumes electricity. Most people will start up their computer in the morning and only switch it off at night, leaving it on all day, consuming power. An obvious solution would be to power down your computer when you go out for lunch and certainly when you leave the office at night. Yes, it may take a while for the computer to boot up in the morning but think of the energy saved.

Modern operating systems have a feature so that if a computer is left idle for a pre-determined time it will automatically enter standby mode switching off the monitor and hard disk, effectively sending the computer to sleep. A few minutes taken to set this up on each



computer can start to save money from day one. The benefit of using standby mode is that the computer will restart a lot quicker than from “cold”, but remember it will still be consuming some power.

Remember that other peripherals such as printers and external hard drives consume power. Turning these off, especially at night when they are not needed, will also help you save money.

In larger technology environments periodic maintenance is often undertaken over night so that it does not inconvenience the end user and therefore turning the computers off at night may not be encouraged.

Printing

20 years ago computer vendors were foretelling the death of the printer as we entered the age of the paperless office. Clearly this is not the case as we simple humans are often better at interpreting data from a piece of paper than we are on a screen. Accepting that printers will be with us for the foreseeable future there are some steps we can take to reduce the cost of printing.

Recycling printer cartridges is an obvious measure as is using recycled paper or maybe a paper of less thickness or weight. Double sided printing is also a great way of saving money as is encouraging printing only when it is absolutely necessary. Once you have printed out documents that you no longer need recycle the paper appropriately. If it is blank on one side and not confidential in nature then use the blank side as note paper, so at least you are maximising the use of the paper. Some e-mail users have a small signature encouraging the e-mail recipient to think before printing out a message.

Technology Hardware

Most computers are underutilised. Their hard disks are often half empty and their central processor is only busy for a small fraction of the working day. Unfortunately the energy a computer consumes is pretty much the same if it is busy or quiet as it still needs cooling and the monitor still needs powering. To deal with this issue there is a move to consolidate hardware so that fewer computers are being used but those that are being employed are working at their maximum potential – a process referred to as virtualisation. This saves money, space and energy. If you look around your office, take a note to see if there are computers that may be under used and consider consolidating them onto fewer physical devices.

The recent movement towards software as a service (SaaS), where key software is hosted remotely, is also beneficial, both for the environment and in terms of cost.

How can Not-a-Geek assist?

Environmental issues can be complex and very involved; the first step is to understand the current impact your technology has on the environment. Not-a-Geek can perform a simple “carbon foot print” audit to help you take the initial steps towards power cost savings and delivering benefits to the environment at the same time.

Stage 2 – Technology Acquisition

Acquiring technology assets and services involves executing the recommendations developed during the Assess and Identify stage of the TLM process and includes;

- Procurement of assets
- Logistics planning
- Finalisation of financing

To simplify this stage, many businesses outsource some, if not all, acquisition-related tasks. A common practice is to have a technology solution provider project manage the acquisition, deployment, and implementation of the technology. The financial planning model is also finalised during this phase. The scenario that significantly minimises a business's risk is to have a contractor purchase the infrastructure and recover the costs over the life of the contract using agreed-upon pay-for-use billing metrics.



Lease or Hire Technology

What Is A Lease or Hire Agreement?

It is always tempting when starting a business to go and buy the latest and greatest computer, but unfortunately the relentless onward march of technology will see that investment becoming obsolete within a few years as more powerful computers become available.

If you hire or lease technology equipment you pay a regular monthly or quarterly fee to the owner of the hardware over a period of time. Once this hire period has expired you are able to renegotiate the deal and upgrade your equipment to the latest version at the same time.

The cost of leasing technology does vary. A business computer may cost around \$15-\$45 per week, ex GST, for a 3 year contract. This includes an operating system and business software. You may be able to purchase the equipment at the end of the hire agreement for a nominal fee and some companies offer an 18-month rolling hardware upgrade to keep the computer up to specification.

Keeping Your Capital

Keeping your eye on cash flow and expenditure is vital if your business is to remain solvent. A reasonable quality office computer will cost in the region of \$1200 - \$2400, which can be a lot of money to a start up. By having a hire agreement the cost of the computer falls under a different accounting section – operating expenses. Whilst this may be a paper accounting exercise it does change your company financial profile. Many manufacturers operate lease schemes so that you can go directly to them to obtain the computers and finance agreement in one go. This saves having to organise a loan or overdraft with your bank or finance provider.

3-Year Refresh Cycle

Most technology companies suggest a 3-year upgrade cycle for desktops and possibly a 5-year cycle for servers. Software can change as frequently as every 2-year however extra care has to be taken when managing such a short period refresh. That means that a lot of your technology investment is assumed obsolete after a short period of time.

A word of caution here, just because a manufacturer says their hardware or software is obsolete does not necessarily mean that you should upgrade. Many businesses quite happily run on technology and software that is several years old, but there are support issues with older computers, which can negatively affect your risk strategies to such an extent it may be more beneficial to change the technology every 3-years.

Computer equipment depreciates quickly. Within 3 or 4 years your \$2400 computer is worth nothing as a financial asset. This means you have thrown away another \$600-\$750 per year per computer. As your business grows so will your depreciation costs.

Cost of Ownership

Buying a computer is the first major cost of ownership, but many people forget there are ongoing costs associated with computers. On a regular basis you will need to perform periodic



maintenance of your computer, keeping it free from viruses and other malware as well as keeping the software up to date with patches. This cost may be small if you have one or two computers but as your business grows you may see the management of computers quite burdensome. In many cases it results in the hiring of technical staff to keep the computers running.

Some leasing companies offer ongoing support and maintenance of their computers out on customer sites. This takes the strain away from you and maximises what you pay for.

Returning Old Equipment

Once you have finished your hire period your equipment will need to be returned to the lease company. An issue that you will need to address is the safe management of data you have stored on the computer hard disks. This will need to be transferred to your new equipment and the old disks cleaned.

Remember that deleting information on a disk can be reversed with some fairly simple and publicly available tools. Therefore to safely sanitise data from a disk can be a time consuming process that will need to be done professionally.

Remember that you can never be too careful when removing old data.

How can Not-a-Geek assist?

Partnering with IBM Global Finance, the world's leading technology financier, you're choosing a dedicated partner with the breadth of experience and offerings to provide any financing solution your business may require.

Solutions are available for small businesses with as few as ten employees to the large corporations.

IBM Global Financing stands ahead of the competition with;

- An unmatched selection of flexible financing solutions and attractive rates for your business
- Solutions at every stage of the technology lifecycle--from acquisition to equipment disposal - so there's no need to deal with multiple financing vendors for different needs

Connecting Offices

Introduction

As your business grows you may find that you need to open other offices and put in place some technology infrastructure that allows remote users to connect to the same network. This will have big business benefits as it enables you to share documents and resources across many locations. In the past you may have had to e-mail documents from one user to another, but with an integrated network these documents can simply be copied into shared folders. This type of setup makes backups easier as well, as data from one office can be copied to the other in case there is a problem locally.



This approach to sharing data is very different to that in online solutions such as Google Apps, which uses a shared network resource remotely on the internet. With the solution we are talking about you are responsible for managing more technology infrastructure, the internet simply provides you with the link to connect offices together.

For many smaller businesses this is their first necessary step in running their own technology systems.

Understanding the Basics

In the past businesses would have provided dial up modem access to their internal networks. This was a slow and expensive way for users to connect and lead to the wide spread adoption of leased lines or ISDN, a form of digital telephone line.

With the advent of the internet leased lines fell out of favour as it made sense to connect across this growing public network. Unfortunately data sent across the Internet is open to abuse by hackers and others that wish to eavesdrop on the communications, so a business should be secured.

A virtual private network (VPN) enables remote offices to connect using the backbone of the internet but with a secure “tunnel” between computers. This removes the need for expensive dedicated leased lines and means that users can connect from their home, remote office or on the road with their laptop, to the corporate network safely and securely. Data being carried across a VPN is normally secured using very strong encryption.

Whilst broad band is now available to most businesses care should be taken when designing an inter-site solution. The amount of un-contended capacity on a link will vary from the advertised headline rate offered by the vendor. Any variations in this capacity can have disastrous effects on your inter-site network.

Installing a VPN

This can be quite complicated, depending on how interested you are in setting up computer systems, in summary;

- A minimum of a broadband connection to the internet.
- You will need to ensure that you have a private, non-routable IP address range for your internal computers so that they are isolated from the wider internet. Your external



router interface should be a static IP address available from your ISP. If you cannot obtain a static IP, for example you are using a wireless connection, and then consider using a service like Dynamic DNS to register the IP against a domain name, for example 123.456.789.123 is associated with www.mybusiness.com.au.

- A firewall needs to be configured and monitored to protect the internet connection.
- It is better to have a site-to-site VPN rather than have many VPN tunnels for each end user.
- You will need to install VPN hardware routers (VPN software on a server is generally not advisable).

Is A VPN For You?

A VPN is not going to be a suitable solution for every business and you will need to take a detailed look at your specific requirements. Here are some general pros and cons that you may wish to consider;

Pros

- Secure and reliable
- Cost effective medium to long term
- Provides good, flexible support for a growing business
- Enables remote users to access and share company data quickly and easily

Cons

- Can be difficult to configure
- May need external assistance to setup
- Requires a reliable and “fast” Internet connection. Be careful if selecting consumer grade public networks – if your business is reliant on inter-site connections you may have to consider a private (leased) network.

How Much Does A VPN Cost?

Pricing a VPN solution is difficult as a lot will depend on individual requirements. VPN routers can be purchased for between \$150 and \$600 each. If you need professional assistance to install and configure your VPN then you will be charged about \$130 per hour. Most small businesses should be able to setup a VPN solution for under \$1000, excluding broadband costs.

How can Not-a-Geek assist?

Whether small business or corporate, we can help with planning for all your technology needs as your business grows. We can design and deploy a scalable robust network, over a small office or in a restricted wide area network that is reliable and scalable to cover your future requirements.

Stage 3 – Integrate and Implement

Integration and implementation of the infrastructure solution should follow a detailed methodology, mitigate risks, and maximise efficiencies by providing;

- System configuration and desktop image loading
- Asset management
- Design verification and quality assurance
- Onsite or remote engineering
- Project management standardised processes

Technology asset tracking involves more than simply knowing where assets are located. Asset management is important for ensuring technology security and the businesses ability to recover vital assets and information. Effective asset management requires a well-planned implementation of a data repository that stores and manages information on where the assets are located throughout the enterprise. Such asset tracking has become more difficult in recent years due to increases in worker mobility and the prevalence among businesses to take a siloed approach to adding computing assets.

Engineering and project management services are central to the success of any IT undertaking. The successful implementation and integration of technology depends heavily on maintaining the scope definition, mitigating risks, collaborating closely with end users, using resources efficiently, and adhering to the budget. Regardless of the size of the project, to mitigate risks resources with certifications specific to the underlying technology should implement all technology infrastructure components.

Project managers are needed to oversee the entire project and can streamline the process by maintaining a repository of detailed plans that are customized to each implementation as well as by efficiently managing multiple resources and developing a close partnership between vendor and business.



Electronic Document Storage

Introduction

If you have not used e-mail before you will very quickly find it becomes part of your everyday business life. For many small businesses over 90% of external communications are conducted over e-mail as it is a convenient and easy to use tool.

One useful feature of e-mail is the ability to save your messages and file them away for later reference. Some e-mail programs have advanced filtering and sorting tools to enable you to file e-mails away and retrieve them by searching for key words or maybe a sender's name.

The downside of this is that your e-mails will become indispensable, and unless you find a way of organising and backing up these messages any data loss could cause your business a real problem.

Managing messages should not take much time or cost much money. A backup may only take a few minutes, and if you back up data to a memory device or CD/DVD the cost is very small.

Typical E-mail Problems

At some point you may experience one or more of the following e-mail related problems;

- Lack of hard disk space.
- Inability to search for e-mails as your e-mail database grows.
- Problems trying to back up e-mail data.
- Problems trying to retrieve archived data.

Unless you do something about it, your e-mail in-box and sent mail folder will continue to gather more and more data as you send and receive messages. Eventually you will get to the point where you are unable to find previous e-mails because they are obscured by all the data in your system.

You might also encounter;

- Restrictions imposed on the size of your e-mail database by the administrator of your system.
- Restrictions on the size of your e-mail storage imposed by your software.
- Instability – the risk of your e-mail program crashing (and the impact if it does) increases with the amount of e-mail data you have.

Managing E-mail Folders

Most e-mail programs allow you to create folders to contain both sent and received messages. Take some time to come up with a folder scheme that will help you find e-mails when you need them. For example, you might organise e-mails by;

- Clients or customers – but don't create a folder for each individual customer as this often becomes tiresome to manage
- Products
- Projects



Then get into the habit of moving received and sent messages into the relevant folder.

To help you, some e-mail programs allow you to create rules that automatically move e-mails into folders based on rules you provide. This can also be a useful way to remove clutter from your inbox.

E-mail Backups

If you use desktop based e-mail, your messages are held on your local computer. You need to be sure it is being backed up or you stand to lose the lot as the result of a single fault. The way in which you backup your data will vary from vendor to vendor, so it is best to look at specific instructions that apply to your e-mail program.

Web based e-mail, for example that provided by Microsoft Hotmail or Google's Gmail, will be managed by the supplier's own staff. Generally these e-mail stores are very secure as they are fully backed up and managed remotely, but often in a different country.

Backups of your desktop computer should be part of your regular data management program.

How can Not-a-Geek assist?

Whereas storage is a physical entity, storing and managing electronic documents requires a solution that involves a combination of people, technology and processes. We a complete solution encompassing;

- Analysis
 - Identify and document existing systems
 - Analyse for future storage
 - Identify key business objectives
- Design
 - Identify the appropriate hardware and software vendors
 - Identify appropriate procedures and processes
- Deployment
 - Solution deployed, tested and documented
 - End users trained
 - Periodic review of solution and modification as business grows

Protecting your Data from Unauthorised Access

Introduction

Every business has data that needs to be secured. If you are running a business as a sole trader then you do not need to really worry about others seeing any confidential data per se, but there are still risks that should be considered, for example if the computer is stolen or if the computer is compromised whilst you are on the Internet.

The purpose of this section is to highlight what should be considered when you start to employ people who may have access to your computer?

Even if they are not employed to work on a computer they may decide to jump into your seat when you are out and have a browse around the internet or your local data, looking at your confidential information.

Steps to Secure Your Data

The chances are you will already have most, if not all, the equipment and software you need to implement the security measures you decided on in the planning stage.

This section talks in a general sense of the steps required due to the many different products, operating systems and even versions of the same operating systems that are available.

If you elect to have an external person assist you make sure that you allow time for them to;

- Show you or someone else in the business what they are doing.
- Document the security measures they have implemented.

Most access controls are simple to update once you know what needs to be done. In your documentation, make copies of key screens and make notes as you go along so you build up a small user manual that means you do not have to involve someone from outside every time you want to make a change.

As you implement each security measure you should test it is effective.

Security Responsibilities

It can be difficult for businesses to decide how best to manage and implement security controls. In particular, who should hold high-level passwords that provide access to sensitive data?

It is clearly desirable that managers make the decisions about who should have access to what data.

It is also likely that managers will not be able or willing to implement those decisions and will want to delegate that job to a relatively junior administrator. However, what is to prevent that administrator using their privileges to gain access to data they are, themselves, not authorised to see? If that person leaves the company, what is to prevent them creating holes in the security measures that they can exploit later on?



This is generally not an issue in smaller businesses where the chief focus is on preventing external access to data or where you can place a high level of trust in your administrator.

If you are concerned about the access available to an administrator, we suggest you consider;

- Giving the business owner or a senior manager responsibility for changing high-level passwords once they have been created. Those passwords should be kept in a secured place readily available in case of emergency. If the passwords are needed, then either;
- The appointed manager can enter the password
- If they are not available, the password can be accessed and a new one can be created later on.
- Making sure anyone with sensitive data that needs to be withheld from the administrator knows how to encrypt that data with a personal password.
- If there is any concern about the circumstances in which an administrator leaves the business, ask a security consultant to;
- Look for possible security holes.
- Make sure all key passwords are changed.
- Ensure that the business is not locked out from any data or systems.
- Implement some type of segregation of responsibilities. This is the principle of preventing one person having control of the data as well as the data security. For example you may have a database administrator who has complete access to your business data. By implementing separation of duties they will not be able to view the data they are backing up as their role is separate to the security role. This can be a difficult process to implement but may be beneficial if you deal with sensitive data.

How can Not-a-Geek assist?

A primary concern for any business owner is the guardianship of customer and business data from in-creasing external threats to security, and tougher compliance requirements in regulated industries.

Our Managed Audit solution provides the business stakeholder who is responsible for the ongoing effectiveness of the security strategy and compliance audits with peace of mind and keep you one step ahead of potential attackers by giving you a comprehensive way to regularly assess and report on possible vulnerability, configuration and compliance related issues.

Connecting to your business whilst travelling

Introduction

For many people in small businesses it is vital that they stay in touch with customers and partners on a daily basis – even if they are on holiday or away from the office. Fortunately modern technology makes this type of connectivity easier than it has been in the past. Unfortunately some may see this as a bad thing as they are never away from the office, and maintaining a life/work balance is a challenge associated with working in a small business.



What Will You Need To Access Remotely?

First determine what data you will need to access whilst you are away from the office. For example access to;

- E-mail so messages can be sent and received whilst they are on the move
- Data that may be in the office such as sales proposals or customer contact data.
- Internal applications such as an accounts package. Whilst this is possible you will find the solution slow and it does pose considerable security risks.

Services That Allow Access to Files and Applications When Working Remotely

There are many internet services that give you remote access to a computer in the office. You can connect using most popular web browsers. That means, for example, you can connect from;

- A company laptop
- A desk top running at home
- A client or customer computer
- An internet café—although this is the most risky approach

In theory, if you make a remote connection via the internet or a direct connection you can do everything as if you were directly using a computer attached to the office network.

In practice, remote connections work at a fraction of the speed of local office connections, even if you use a fast broadband connection. The slow response times can make using some services tedious and inefficient.

You will, however, be able to;

- Upload and download files (although, of course, the larger the file, the longer you will need to transfer it)
- Connect to services designed for use over slow speed connections. This includes most services that can be accessed via a web browser.

Making secure connections over the internet can be difficult to achieve. For example you will need to create an opening in your office security (firewall) to allow someone to connect into the network.



Note: This approach has a large number of caveats and associated issues with them, notably security concerns when connecting to a computer that is switched on and waiting for connections across the internet. It is strongly suggested that you review your access strategy with a security consultant who can offer advice to help you remain safe and sound.

Alternative Approaches Accessing Data

Some alternative methods to achieve the same thing;

- Ask someone inside to send you a file to an Internet hosted e-mail service
- Store a file on an external service that is available from the Internet i.e. Google Apps

This assumes that there is someone in the office willing and able to do that for you. If there's no one in the office (over a week-end, for example) you will be unable to retrieve files at all.

Collaboration services allow you to create a shared repository of files available via the Internet. For example, if you regularly prepare and send proposals to clients, you might keep all the latest CVs and copies of past proposals in a collaboration service. This would not, however, give you full access to everything available on the office server.

Summary

Despite all of the new technology available to help you access files it is probably better to have an efficient and effective working culture that enables you to take important files with you and not rely on connecting to a remote computer.

With the prevalence of memory stick devices it has never been easier to carry files safely and securely whilst you are travelling. Many of these devices support encryption so your data is going to be safe should the memory stick become lost.

The problem with memory sticks is then keeping your data up to date or synchronised especially if it could have changed on the memory stick and internally on the server during the same time window.

Technology Security Training

Why Technology Security Training Is Important

Corporate Governance and the importance of protecting your data from unauthorised access and inadvertent corruption should not be underestimated. To do this you educate your staff about the importance of securing business data and what they need to do to help with this important task.

In general, you should consider education and training tasks throughout the implementation phase of a technology solution. It makes sense to start the education process early on, but you will have to defer some training until you have set up the data security you need.

It is important that you give security training to everyone in your business and make sure your security policy is clearly documented and available to everyone. This education should also be an important aspect of the business induction for new joiners and the consequences of security abuse should be detailed in the terms and conditions of their employee contracts.

You will need to ensure everyone knows;

- Why security is important and what they need to do about it.
- How to maintain good password discipline.
- Your policy for storing data away from the office.
- How to avoid picking up malicious software infections while using the Internet.

How to Maintain Good Password Discipline

Everyone in the business will need to understand the importance of password discipline. Specifically;

- The need to keep passwords private.
- The need to change default passwords in software and equipment (and document changes centrally).
- Do NOT share usernames and passwords – a breach in policy will be associated with the user name, do not take the risk of collecting the blame for something a colleague did under your user name.
- No one should ask people for their password; and they have the right to refuse to provide it.
- Do not write passwords down or include them in e-mails.
- Any software you have provided to store user ids and passwords securely.
- Methods to come up with memorable passwords. A good one is to come up with two completely unconnected words connected by a piece of punctuation. For example: train+envelope. Now create a mental picture that features the words you chose; for example a train sticking out of an envelope. You might be surprised how easy this kind of password is to remember.
- Being vigilant for any failures of password discipline.

You should make sure people know your policy for using business data on equipment that is to be taken out of the office;



- Which data cannot be taken outside without permission?
- Which data can be taken outside without issue because it is not sensitive?
- How to protect other data;
 - Encryption.
 - Keeping an eye on the equipment.
 - Password protection of equipment.
- How to avoid picking up malicious software infections while using the Internet. For example;
 - Stick to reputable web sites created by reputable businesses.
 - Do not open e-mails that are clearly junk mail.
 - Do not open links in e-mails unless you are sure you can trust the sender to have the expertise not to pass on links to malicious sites.
 - Never respond to junk e-mails

Security Responsibilities for Technology Administrators

- Implement the security measures you decided on in the planning stage.
- Update programs if that is not done automatically.
- Add, change and delete access folder-level and file-level controls (if you need them) and ensure the supporting documentation is kept up-to-date.
- Help people use access control facilities (such as encryption) when necessary.
- Ensure User ids and passwords are created promptly for new hires.
- Arrange induction training on data security and associated policies.
- Ensure ex-staff have their access revoked promptly.

Updating Employee Terms and Conditions

Consider including words in people’s terms and conditions of employment that makes it clear that you expect data security discipline to be observed and that failure to observe those disciplines will be treated as serious misconduct liable to summary dismissal. That sounds heavy, but you need to ensure that you have the ultimate sanction for people that refuse to take security seriously.

You should also consider making it clear that Internet and e-mail access for any purpose other than strictly necessary for their job is a privilege that can be revoked at any time; and that you maintain the right to review and intercept Internet and e-mail use in order to ensure your company’s policies are being observed. Without these protections in the terms and conditions you might find you have no rights to check. You should, of course, obtain legal advice for suitable wording.

How can Not-a-Geek assist?

We offer training cover broad governance and security awareness based on “Corporate Governance of Information and Communication Technology (AS 8015-2005)”. This standard provides guiding principles for business stakeholders on the effective, efficient, and acceptable use of technology. It applies to the governance of resources, computer-based or otherwise, used to provide information and communication services to the business.

Security Policy

Introduction

The chances are that you have been busy writing business plans and have in place a great sales and marketing process. But one thing many small businesses forget to create is a policy that helps you secure the technology used in your business.

By implementing a policy you will have laid out clear lines of responsibilities and will ensure you and your team protect the reputation of your business.

If you follow these steps it should not take you long to build an effective technology security policy.

Objective of a Security Policy

Some very small businesses will see the creation of a security policy as a waste of time. For most sole traders it is not necessary to create a formal policy as you are working by yourself and can be in control of your technology personally. That said there are still some tips that are important for all size of business of all sizes.

For small businesses that employ one or two staff that use company technology as part of their job, a security policy can act as useful protection against bad employee behaviour and get over the claim by an employee that “they didn’t know”.

In some cases you may find your customers and/or suppliers demand that you have a security policy in place that they can review – especially if you may be formally linking into their technology systems.

The growth in social networking and online gambling sites is causing concern to many employers as these sites can be a huge distraction from day to day work. In addition access to certain sites may lead to compulsive behaviour that is beyond the remit or management skill of a small business owner.

The objective of the security policy is to;

- Set the boundaries of employee use of technology.
- Say what is deemed acceptable behaviour when using technology.
- Explain processes and procedures that have been implemented to protect and manage technology.
- Assign roles and responsibilities for staff so everyone knows their respective tasks.
- Explain what will happen if the policy is ignored or deliberately breached.

Security Policy Best Practice

As a business owner and probably managing director you have certain legal responsibilities and expectations. Many of these are outside the scope of this document as they relate to the good management of a business but many related expectations can be laid out in your security policy.

The actual policy will vary from company to company.



Consider including words in employment contracts that make it clear that you expect data security discipline to be observed. You will also need to say that failure to observe those disciplines will be treated as serious misconduct liable to summary dismissal. That sounds heavy, but you need to ensure that you have the ultimate sanction for people that refuse to take technology security seriously.

You should also consider making it clear that internet and e-mail access for any purpose other than strictly necessary for their job is a privilege that can be revoked at any time, and that you maintain the right to review and intercept internet and e-mail use in order to ensure your company's policies are being observed.

Without these protections in an employment contracts you might find you have no right to check what people are up to. You should, of course, obtain legal advice for suitable wording.

In terms of a general security policy ensures good general behaviour by;

- Banning access to unsavoury sites. This could include online auction, gambling and social networking sites. Tools and technologies are available to help you with this task if it is a significant concern.
- Banning all sharing and downloading of copyright material such as songs, films and videos.
- Letting people know their internet access is being monitored and activities will be reviewed. Again there are tools to help you with this if you see it as a significant problem.
- Telling people to protect their passwords and enforcing password changes every so often. There are tools to assist with this.
- Clearly stating what will happen if anyone breaks any of these rules.
- Ensuring e-mails have an automatic disclaimer about the content.
- Stating how e-mail communication is to be conducted – maybe using the “letterhead” principal. Everything that you write in an e-mail is as binding as a letter on your official note paper.
- Letting staff know your acceptable use of Instant Messaging, if you permit it at all.

It is important to consult with people over the security policy and explain why it is so important. After all it is everybody's jobs and reputations on the line if someone transgresses. It is also an idea to periodically check the policy to make sure it is keeping up with the latest innovations and technologies.

How can Not-a-Geek assist?

Our customisable policies and procedures save you the time & effort of creating them yourself. Select from a wide range including;

- Information Sensitivity
- Acceptable encryption standards
- Router, server or desktop security

E-Mail Policy

Introduction

If you have one or two people working in your business that have access to e-mail it is important that you supply them with guidelines on what is acceptable use of company e-mail. Although this may be seen as a bit excessive, it provides you both with guidelines that should ensure a productive work environment.

As a business owner it is obviously important that you set an example with your own use of e-mail.



Why Should I Bother With an E-mail Policy?

A good way to think of e-mail is that everything that is released from your business e-mail account can be held to represent you and your values – and no business would want to be tarnished following the inappropriate use of e-mail.

- If you do not provide people with guidance they could accidentally damage your image.
- You may find guidance could improve people's productivity.
- Unless you have an e-mail policy, you will not be legally able to monitor e-mails – even if they've been sent under your business name!
- E-mails are subject to law. An e-mail policy is a useful document that will help educate employees on good e-mail practice and what is allowed on company premises.

What Should My E-mail Policy Contain?

The precise content of your policy will vary, depending on who has access to e-mail and the type of work they are expected to do. As a guideline the contents should include;

- A declaration that e-mail is provided as a privilege that you are allowed to withdraw or restrict at any time.
- A declaration that use of e-mail is subject to allowing your business to review the content of any sent or received e-mail at any time.

You might also want to lay down policies about;

- Personal use.
- Authorisation needed before sending e-mails.
- Responsibility for filing copies of sent and received e-mails.
- Responsibility for backing up e-mail databases.

Unacceptable E-mail Behaviour

What may be unacceptable to one business may be acceptable to another. As a guideline here are some generally unacceptable behaviour when using e-mail;

- Use of company communications systems to set up personal businesses or send chain letters.
- Forwarding of company confidential messages to external locations.



- Distributing, disseminating or storing images, text or materials that might be considered indecent, pornographic, obscene or illegal.
- Distributing, disseminating or storing images, text or materials that might be considered offensive or abusive, in that the context is a personal attack, sexist or racist.
- Accessing copyrighted information in a way that violates the copyright.
- Breaking into the system or unauthorised use of a password/mailbox.
- Broadcasting unsolicited personal views on social, political, religious or other non-business related matters.
- Transmitting unsolicited commercial or advertising material.
- Undertaking deliberate activities that waste staff effort or networked resources.
- Introducing any form of computer virus into the corporate network.

Managing Unacceptable E-mail Behaviour

If a member of your staff has violated your e-mail policy then you will need to manage the situation as per their contract of employment. As a small business you will probably not have a dedicated HR department so you may need to get advice from an external legal company if the problem is significant.

How can Not-a-Geek assist?

Our customisable policies and procedures save you the time & effort of creating them yourself. Select from a wide range including;

- E-Mail use and guidelines
- E-mail retention
- Electronic record keeping
- Information sensitivity

Electronic Documents and the Law

Introduction

Almost all of civilisation has relied on physical information storage – but the amount of information a business is now exposed to is huge. We are living in exponential times ...

It is estimated that;

- A week's worth of New York Times contains more information than a person was likely to come across in a lifetime in the 18th century
- 4 Exabytes (approximately 1, 073, 741, 824 DVD, with each DVD containing 350, 000 pages of information) of unique information is generated each year – that is more information than in the last 5000 years!
- 98% of all business communication is by e-mail

How many e-mails do you receive each day? The chances are that not all are those you want and a high proportion includes spam messages. If you use e-mail in your business then you need to understand the legal issues surrounding e-mails.

By understanding e-mail and the law you can hopefully save your business money and avoid legal problems.

This section does not constitute legal advice. It is therefore strongly recommended that you seek the services of qualified legal professional to deal with your specific case.

Document Revolution

With more information now stored as electronic documents and the ease with which these documents can be stored, the business discipline associated with managing that storage is getting weaker.

Why bother to manage something, which takes time and resources, which therefore costs money when I can simply copy it all to an external USB disk that can store 25 DVD of information for \$150?

The more information we have then the harder it is to find something later. Should your business be subject to a legal action and the relevance of that stored information has to be ascertained by a legal professional then the costs could be substantial. One estimate suggests it would take an average lawyer 25 weeks to review such a volume of information at a cost of \$394, 000.

There are 80+ laws that impose retention and destruction obligations on corporate Australia. A good starting point to identify what obligations may apply to your business can be found in the following documents;

- Guidelines for the management of IT evidence (Australian Standards, HB 171-2003)
 - Aims to bring an Australian law perspective to requirements for judicial or administrative proceedings. Whilst the document is aimed at maximising the potential for evidence to be accepted by a court, it also presents processes that



are international best practice in many other jurisdictions. It demonstrates incident handling, administrative procedures, operational procedures and electronic evidence processing systems that are applicable to electronic documents.

- AS ISO 15489.1-2002 Records Management Part 1: General
- AS ISO 15489.2-2002 Records Management Part 1: Guidelines
- AS/NZS 7799.2:2003 Information Security Management Part 2
- AS/NZS ISO/IEC 17799:2001 Information Technology – Code of Practice for Information Security Management

Disaster Recovery and Business Continuity Management

Introduction

Disaster Recovery is NOT simply having a backup tape!

Unfortunately disaster can strike at any time. The media are often full of reports of local disasters and graphical images on television of floods and fires. Those directly involved are often faced with the complete loss of their homes as well as their livelihoods and it may take some people many years to get back on their feet.

From business perspective disasters that strike may not be quite so dramatic but can still have a terrible local effect?

- A mains water supply fails and floods your office
- Your house catches fire, taking with it your home office
- The industrial unit next to you has a fire which engulfs your premises as well
- All of your computer equipment is stolen one night
- You get a catastrophic computer virus that destroys your network and computers

All of these are disasters in their own right. Not all of them would make the TV news but for those involved the effect is the same – the business cannot carry on trading and there could be catastrophic loss of business data.

Of course proper disaster management involves more than technology issues and needs to cover other areas including people, premises, public relations, supply chains and partner relationships. These other topics are outside the scope of this guide but readers are advised to investigate disaster recovery issues in these areas.

By preparing for any disaster you will save both money and time for your business.

Planning For Disaster

Many large businesses have sophisticated plans to relocate thousands of employees and their associated support systems to new offices within hours of disaster striking. They spend a lot of time and money providing additional computer systems that contain copies of ongoing work that can be brought on line quickly in the event of a problem.

In smaller businesses we don't have such luxuries but the planning process is just the same, albeit on a smaller scale. To start the processes consider the following questions;

- What technology is critical to your business?
- What systems could you manage without?
- How long could you trade for if you lost your critical technology?
- How will you keep running the business if you lost our office facility?

Business Continuity Management / Disaster Recovery is not that difficult. Just think through some of the issues you may face and put them into perspective based on the likelihood of an



incident. For example if you live on top of a hill you may not be flooded but your home office may be damaged due to high winds. Ultimately the same problem needs addressing – how can you continue to trade with limited or no IT systems?

Documenting your recovery plan is important. Remember to keep a copy in a printed format safe and secure from the main business but available to all key team members.

Now you have the plan—PRACTICE IT—don't let the plan just sit on a shelf gathering dust. Make sure everyone is aware of their responsibilities and test the plan and periodically reviewing anything that went wrong and updating the plan accordingly.

The Importance of Technology Backups

If there is one simple lesson that needs to be learnt from this guide it is the importance of computer backups. A backup is a comprehensive copy of your computer data that can be restored (i.e. re-loaded) in the event of your computer systems failing. By restoring backed up data you can carry on operating your technology as if nothing has happened, from the point in time that the backup was taken.

In summary:

- Always backup your critical data on a regular basis. Think how much data you are prepared to lose – 1 hour? 1 day? 1 week? This will give you a guide as to how frequently you should back up your data.
- Always check that you can restore from backed up data. Practice restoring data so in the event of an emergency you are able to cope with the additional pressure.
- Always keep your backed-up data secure and off site. If you have premises then take the backup home with you. If you work from home then place the backup somewhere safe and secure away from the home office.
- Keep your original software and licence keys safe and secure.
- Having a backup is one thing but how and where will you restore if the backup technology has been destroyed?

In the event of a Disaster ...

First, do not panic. After all you have planned for this and have decent backups ready to be deployed. Of course disasters will vary in magnitude but the same process of ensuring the safety of you and your team would always take priority over any technology recovery. Assuming that you are all safe and well you need to start the business recovery phase.

Access your recovery plan, sit down and think through the actions you need to take.

From a technology perspective you may need to configure new computers before restoring your back up data. This can be complicated so getting help from a vendor may be advisable. Assuming you have the original software and backups available then this should not take too long. The precise steps to achieve this are outside the scope of this guide as they can be quite involved but followed logically are not too difficult.

You may need to consider a communications plan to customers, suppliers and partners so they are aware of your situation and hear it from you rather than the local papers. Done correctly you may be surprised at the level of support you receive.

Disaster planning need not be difficult and it follows best business practice of being prepared to deal with unforeseen circumstances.

How can Not-a-Geek assist?

Our managed services solutions help mitigate the risk of a disaster happening in the first place. With 24x7 monitoring of your technology we can often identify a problem before it becomes an issue and thereby allowing for preventative maintenance to be undertaken.

Of course issues can still occur, so with our comprehensive managed service solution we also design and implement business continuity plans so that your business can continue even when the technology stops.

Stage 4 – Support Services

Vendors must be able to provide post-implementation support services that enable high infrastructure productivity. These services, such as on-going proactive maintenance, are critical to keeping the technology infrastructure operating in its optimal state at all times.

Support services should also include;

- Configuration and change management, technology restoration, and software upgrade maintenance agreements to match the intended lifecycle of the technology including appropriate service level requirements. These are often integrated into pay-for-use contracts as part of the service.
- Warranties that extend or uplift manufacturer standard (1 year) warranties
- Proactive incident monitoring, technical phone and onsite support, and parts replacement
- Monitoring capabilities that include the ability to accurately manage the state of the asset and its support history
- On-going collaboration between the business and the vendor provides a forum to discuss how new technologies can accelerate technology infrastructure modernisation, security, and performance objectives.
- Financial implications and business benefits should be evaluated to ensure that budgets and objectives will not be adversely affected.
- Periodic reviews to discuss performance metrics ensure that the technology infrastructure continues to meet agency technical and business objectives.



Support Options

There are a number of ways in which you can support your technology;

- **Learn about technology and support yourself**—this option may be useful if you have a very small business and you have an interest in technology. You will need to decide if supporting technology is where you should be spending your time rather than managing your business. Every minute you supporting technology computers you are not growing your business.
- **Employ a person to be your support technician**—for small businesses with less than 25 or so people this is not an option, unless you have demands on technology that are out of the ordinary. A full time support person will need a salary between \$40,000 and \$60,000 per year.
- **Use another member of staff**—sometimes you may find a sales person or production person has an interest in technology outside of work. If you trust their judgement and expertise then you may be able to get them spending some of their time doing technology support. Consider what impact this will have on their other role, as ultimately they will only have so many hours each day.
- **Use a third party**—as you would call a plumber to fix your water pipes calling in a technology vendor is probably the best way of dealing with technology problems. It would be better if you have a regular support agreement with a third party as many of them will allow so many hours of onsite support as part of the agreement. Even if they are not called to fix a specific problem, they could still come along and carry out proactive monthly system maintenance.



Selecting a Support Company

You will need to understand precisely what you want from a support company;

- Do you want regular maintenance?
- Do you want onsite support (i.e. someone coming to your office/home)?
- What technology are you using? Is it out of the ordinary?
- What skills do you have/your team have?
- Are you able to explain any problems easily or is technology all new to you?
- Do you want this company to supply your hardware and software? If so you may be able to negotiate a discount on a support contract.

When you buy technology you will often receive an offer of support from the vendor. Some of this may cover a free of charge period, which could be cost effective. Consider extended warranties as they may also be a useful safety blanket.

The internet is also full of help and advice – which is fine if your computer is still able to connect to web sites. You should also consider if your time is, again, best spent doing such support work.



Stage 5 – Technology Refresh

Under a traditional capital acquisition plan, funds that were allocated for refresh may go to other departments.

With TLM, the funds for refresh are secured since a strategic plan is documented being followed by the business. This enables the upgrade of technology infrastructure to keep up with increasing user demands and applications and prevent system failures and service interruptions.

Consultants and certified engineers should conduct an evaluation of assets and systems to determine the best application of technology for specific business needs and environment. Once this is determined, a schedule for replacing technology with updated assets, services, and manufacturer changes is developed.

Refresh strategies are driven by business objectives, including security, financial, and growth requirements and vary by technology category. For example, desktop and mobile platforms have a limited useful life and upgrade potential. In contrast, larger server platforms and storage arrays incorporate extensible, modular platforms that enable them to be expanded or upgraded with processor and board refreshes, extending their useful life.

Establishing a refresh schedule based on historical performance and usage requirements in 3 to 5 year cycles will improve overall technology infrastructure performance by reducing downtime and decreasing costs.



Stage 6 – Asset Disposal

The disposal of retired assets is addressed during the planning stage and is a standard offering of most vendors. Some businesses may choose to cascade technology to administrative or other business units that do not require the most advanced computing platforms. The business should assess the true cost of repurposed technology such as security risks, patches and replacement parts, and out-of-warranty repairs.

Most businesses do not have dedicated asset disposition capability nor do they benefit from the sale of retired assets. Therefore this phase can be outsourced to a contractor, relieving the businesses of the responsibility to manage their own asset disposal when equipment reaches end of life.

Special attention needs to be paid to data security during this disposal process. Regardless of the disposal technique, disk drives will need to be either erased or physically destroyed. If the asset is to be redeployed elsewhere, a new standard image should be applied to the equipment before redeployment. In addition to coordinating the disposal of computing assets with internal departments, it is increasingly important that computing assets are disposed in a safe and environmentally friendly manner.



Recycle Old Technology

Upgrading: Is It Worth It?

For many small businesses it is important to save as much money as possible - after all any expenditure will have an effect on your profits. With computer hardware it is very tempting to buy the latest products each year as they look really good in the office. But is this a wise course of action? In reality a lot of computer hardware can be effectively recycled and its life extended by clever upgrading and redeployment.



Upgrading and Reusing Your Current Computer Infrastructure

As computers become more and more powerful many people find the computer they use is more than capable of running their day to day software. This means that computers can quite easily be cascaded down an organisation so that as much value can be squeezed out as possible. For example if you need to have the newest high end computer to run engineering software each year why not cascade your old computer to someone else that you are working with that does not need such a high specification?

Some small companies may keep a pool of old equipment safely locked away for use in emergencies. For instance if a laptop is stolen or lost why not reissue an old laptop to enable the person to carry on working?

The use of good backup systems (maybe using a central server) will enable someone using a temporary computer to download their files and carry on working - hopefully without much data loss.

What Can Be Upgraded?

One obvious candidate for an upgrade is computer memory or RAM (Random Access Memory). New operating system software consumes a lot of this memory when it is running, often leading to poor performance on computers with low amounts of memory. Many computers have got the capacity for you to add additional memory quite simply. In practice it is very straightforward and can take the matter of minutes to upgrade a computer's memory as the new RAM is slotted into place.

In some computers it is possible to upgrade the central processing unit (CPU) which is the brain of the computer and can be a bottle neck if the CPU is unable to run the latest computer software.

Likewise it is possible to upgrade hard disk drives in a computer to add additional storage space for files and documents.

These upgrades are simple and can be done in a few minutes, possibly saving you considerable expense in buying a new computer. The cost is not that great either. For example 1GB of RAM will cost about \$100.



When Not To Upgrade

There are many instances when it is not cost effective to upgrade your computers. If they are more than 5 years old the chances are that the technology they use is more or less obsolete.

In this case you are better off cascading the computer to someone else in the organisation or arranging for the safe disposal of the computer.

If an upgrade is going to take more than an acceptable time then you may be better off disposing of the computer and purchasing a new one.

How to Dispose Of Your Old Computers

There are a number of computer recycling projects that will take your old computers and refurbish them for use in charity projects. It is good to support such activities but you **MUST** ensure that all data has been removed from your hard disk drive.

Just deleting the data is not sufficient and even a reformatted drive may not be safe if it contained sensitive or confidential data.

If you are in any doubt get the help of a professional company who can sanitise your disk for you. This process will destroy the data on the hard drive in a certifiable way.

Do not be tempted to throw away old computer equipment in your rubbish bin. In fact many local authorities will not take old computers as part of general waste as they contain so many harmful materials. It is important that we are all aware of our responsibilities and avoid IT equipment ending up in general land fill.



At Not-a-Geek we are business people just like you.

We understand that technology must provide a benefit to your business and not present more headaches for decision makers.

Our solutions reduce the risk of technology failure whilst at the same time reducing the cost of your technology support.

These solutions are not just for big business and corporate, they can benefit not-for-profit and small-to-medium business alike.

We support and take care of your technology, allowing you to invest more time on your business.

Our exposure to technology areas in many industries over the years has developed a broad set of practical skills that allows Not-a-Geek to offer a full out sourced technology management service.

As we operate with a practical ethic, we are not swayed by “gizmo's” and we have a firm belief that “if it isn't broke don't replace it”

How do you know if it's not broken if you don't manage it? So just like the trusty car, sometimes “oil changes” and “tune ups” are required for technology too.

Not only can Not-a-Geek manage your technology, we can provide the holistic suite of services to cover all aspects of technology management, including;

- Managed services
- Computer and Network Consulting
- Planning and Design
- Procurement
- Implementation and Maintenance

Visit our www.not-a-geek.com.au for more information.

Not-a-Geek Pty Ltd
5 / 75B Forrest St
Geraldton, WA, 6530
08 9964 9648