



Guidelines to reducing cost and hassles in IT for small and medium business:

5 key principles

Computer networks and IT can be very frustrating. Why can't they just work, right? Mostly, it's because things changed whilst you weren't looking. You had to spend your time getting operations working, seeing clients and dealing with staff rather than worrying about IT best practices. So what are those things that changed?

Most of your computer systems are in place because you needed them to respond to a business demand of some sort. You needed email to communicate with clients or staff and a basic bookkeeping package to keep track of the finances. Everything else was on a spreadsheet until that became cumbersome, and then an accounting package with some customised features came along, and so did a small CRM application to try and keep client details in one place. Or perhaps you had to install a program to perform specialized tasks like control some machinery, track shipments, collect data and so on. One of your suppliers insisted you use their program to place orders electronically, or a service provider installed an application to manage something or other. You needed a firewall because your IT guy said so, and then a branch office was setup with a VPN connection over the internet. Somewhere along the line a database like SQL was installed on a server, and more users were added along with the necessary network hardware, cabling, and servers. Before you know it, you're sitting on a bird's nest of information and systems.

For most small and medium companies like yours, email, applications, notebooks, internet, databases, accounting, CRM, ERP and all these digitised things have worked their way into the core of your business. They've become an essential part of your day and continue to become more important either because you need them to perform operations or they've become strategic. Either way, your network is more than the bunch of cables and computers it used to be.

The bad news is that you have to accept that this has happened and face the problems head-on before they start to slow your business down. The good news is that you don't have to take the approach of big corporates and hire IT staff or get some IT giant to throw confusion down with a hefty bill. There are a few simple tasks that you and your support company can undertake that will make a big difference in just a few weeks to a couple of months.

About us

Network Configurations specializes in taking the worry out of IT for small to medium sized companies. Our INSIGHT Managed Services solution was developed specifically to simplify technology support for companies with limited or no internal IT resources and help them get more out of their computer networks. Comprising the key pillars of network support, email management, IT security, data protection and license management, the solution is backed by over 10 years of experience and over 30 skilled experts delivering services remotely and onsite.

Leaders in Managed Services for Small & Medium Sized Businesses





Principle 1: Standardise

Your computer network is most likely a jumble of systems, office versions, computer names, conventions, suppliers and platforms that could be impacting your business operations or is at least threatening to do so soon. Applying standards makes your systems more predictable and speeds up troubleshooting so that downtime is not extended due to ridiculous things like not knowing what 'that' server setting is. For your computer network system to operate like a system in needs to have standards applied just like any other system, and anyone needs to be able to quickly understand it to troubleshoot problems.

Steps you can take

- *Draw up a list of applications* that are normally required by each person or, if you have departments, then each of those. Keep this list with relevant settings and information in a central location so that a 'base system' for installations can be created where you can ensure the same versions and settings are applied to everyone. For the technically advanced, you can consider creating group policies.
- *Standardize computer names and network addressing* to facilitate faster troubleshooting and easier problem resolution. Create a document with this information so that it can be accessed by your service provider or technical support. You're not looking for perfection, just a good working standard, like "company_PC-type_number-user"
- *Look to create standard settings around major applications* – trying to cover everything is not feasible for SMBs. Email mailbox settings should always be the same and to keep uniform communication you should consider using a product to automatically add a company approved signature at the server level to every email. Antivirus applications must always be the same product, product components, version and signature version. Internet settings should be centrally standardized. Your line-of-business applications will have some standard requirements so get these from the people who supplied and installed it so that you can replicate an installation.
- *Business data should be kept in the same place.* You need a "Users" folder that all user data is stored in whether it is saved there directly, via a mapped network drive on your computers, or by applying folder redirection to the "My documents" folders. You'll also need a "Shared" Folder for centrally sharing reports, application output, common information and so-on. Then consider some specific needs – perhaps a management folder with security that only management can access, and a downloads folder for internet downloads. By doing this you can secure your information and make sure it's being backed up.
- Backup sets need names that indicate what they are (e.g. COMPANY_SQL_DATABASETYPE_01-DAILY) and these should be grouped around data type (Business critical databases; business critical information; user data; shared data; etc.) You can then apply standard schedules to the types e.g. SQL data must be daily and offsite, user data daily incremental, shared folders weekly full etc. You can also see at a glance exactly where you might be at risk.

Questions you can ask your support company

- What IT standards have you created for my business and where are these documented and stored? How have you applied the best practices?
- How do you specifically ensure that my data is always being backed up?
- What measurement benchmarks have you defined to ensure my security, communication and disaster recovery needs are met?
- How do you check on site standards and how often?
- What are the key components of my computer network (including software) that directly affect my ability to do business?

Leaders in Managed Services for Small & Medium Sized Businesses





Principle 2: Automate

Performing tasks automatically is a primary driver behind reducing support costs. By using the correct methods, the performance of systems, security of the network, availability of critical business applications and even the management of risks can be drastically improved without having to increase the hours you get billed.

Steps you can take

- Create scheduled tasks to perform routine system maintenance – and there are many ways to do this. Even windows task scheduler can help you. Things like cleaning up temporary files, doing disk defragmentation and checking for disk errors are a good place to start. There really is a ton of value to be had even with these basic steps.
- Review your support calls – are there tasks that keep getting repeated? Is there fire-fighting that could be avoided? Get your support company to write some basic scripts to restart services that either fail often or are critical to your business. In fact, many problems are solved by following the same steps, so find someone who can automate those by kicking off a process based on set conditions
- Windows updates and application patches are important and must be done automatically as doing so manually is literally impossibly time and resource intensive. However, some can be problematic to customised applications and even system reliability, so most people go with an “always on or always off” approach. This is where you need tools to assist with managing automatic patch updates. Your support company should be able to assist with one they are trained in, but companies such as GFI, Lumension and Shavlik seem to have good offering for SMBs if you want to do it yourself. If you’re going large, look at n-able, Kaseya and LabTech.
- Identify critical business data and implement a system to move it off-site without the need for manual intervention. If you’re swapping out hard drives or still dealing with tape, your risks are too high and the manual requirements leave it open to human error (which you only find out about when it's too late).

Questions you can ask your support company

- What reports can you show me that my systems are running at optimal levels in terms of patches, updates and performance?
- How do you apply controlled Windows or Office patches and security updates without disrupting my operations?
- What testing criteria or application criteria have you defined to ensure patches don't break my systems?
- How do you ensure my data is protected without the need for manual tasks?
- What routine maintenance tasks have you implemented to reduce the need for ‘fire-fighting’ computer problems?

Leaders in Managed Services for Small & Medium Sized Businesses





Principle 3: Monitor

What if you could get ahead of the game by being proactive and using live monitoring of your computer network to *prevent* business interruptions rather than frantically *reacting* to them? Add proactive maintenance, remote support and system optimization and you can get quicker fault resolution, better performance and greater longevity from your IT investment, not to mention more efficient staff.

Steps you can take

- Create a proactive support schedule that can be used as a checklist of manual tasks that must be done weekly or monthly. Sign it off every time to ensure it is actually being done. These tasks should include, at the very least, server management console lists, UPS communications, event logs, hard drive/RAID status, Mail database size, backup schedules and status, services and anti-virus patterns.
- You need an early warning system against failure – set up alerts for critical conditions such as low disk space, high memory usage, SQL transaction problems and CPU Usage using free or paid for software tools. Once again there are a ton of options available (check out [this comparative list](#)), but your support provider should have a preference that they can help you with.
- Alerts are useless without a means to respond to them, so get these alerts into a ticketing system such as the free helpdesk package Sysaid. If you have no internal technical skills, make sure your service provider handles these through an SLA driven operations centre or helpdesk to avoid them simply being ignored.

Questions you can ask your support company

- How often to you do you proactively maintain and control my systems and where is this documented?
- What conditions and thresholds alert you that there is a potential problem that will impact my business?
- How often are my systems cleaned and optimised and what specifically is done?
- What hardware and software do I have installed and how often is this information updated?

Leaders in Managed Services for Small & Medium Sized Businesses





Principle 4. Document

Many companies have experienced the "Great IT Guy" – the whizz-kid who always knows how to fix problems. But when the IT Guy is unavailable, the simplest problem such as not knowing a password can keep a business off-line for hours and cost thousands in needless support charges. Recording important information is crucial to delivering consistent service and timely fault resolution even if the initial time investment is high. If you want to get a handle on the types of documents you need and methods you must follow, read "Work the System" by Sam Carpenter (Greenleaf Book Group, 2009).

Steps you can take

- Produce a network diagram and server diagram. This is a great way to see what's happening at a glance, and also a good place to store network IP addressing information, what application are running on what server and so on. This is typically your best place to start to get a handle on where you need to get more information.
- Create a secure database where site information such as passwords, service providers, directory, Internet, application, firewall, email, and other data are stored. Consult your network and server diagram and run through each system in your mind to see what information would be critical to have on hand: Who do I contact? What details will they need to help me? Where is additional info stored? Do NOT simply think your service provider has them because chances are they are simply written on a whiteboard or in the back of someone's notepad and that's not good enough.
- Get some forms going. Create a new user setup form with some tick boxes to indicate what they need in terms of hardware, software and network access. At the very least, include fields for their name and contact details, what type of computer they need or if they're taking over a previous computer, how they will access the network (locally and remotely), where they will print to, where they need to store their documents and what their internet requirements are. Also be sure to document your backup times and what folders are being backed up to where – then make sure this gets signed off if any changes are made. And if you've ever battled with downtime due to work done on your network, create a change control form and procedure to avoid changes being made to infrastructure or applications. We've created many of these already so if you need samples just let us know.
- Every time a problem is solved, record the steps taken to resolve it to speed up play next time it happens. Publish these in a knowledgebase or wiki for future reference if you can. Or ensure that ticket resolution is saved to some sort of database by your support company, otherwise you're back to having that one 'great techie' that knows how to fix the things on your site.

Questions you can ask your support company

- What information have you recorded about my site and where is this kept?
- How are you documenting the steps taken to resolve faults and can all your engineers access this?
- What happens when an engineer leaves your business?
- What is your process to ensure no-one makes changes that result in business downtime, and can this be audited if needed?

Leaders in Managed Services for Small & Medium Sized Businesses





Principle 5: Evaluate

Until technology adds advantage to your business in some way - perhaps through competitive edge, process efficiencies, or ways to reach new customers - it is simply another cost at the end of every month. In addition to this, you also need to know what the cost associated with *not* spending on technology is in terms of risk and potential downtime. With regular reviews of your technology and some forward planning you can make better decisions and find ways for technology to truly support your business objectives. At the very least, you can ensure that you're not spending on preventable problems. Like the old saying goes, you can't manage what you can't measure.

Steps you can take

- Create a 'map' of key areas of IT (uptime, email, security, data backup, main applications, internet, hardware, network and software compliance) and review these areas regularly to evaluate risk and cost. Turn this into a meeting agenda to discuss with the company providing your IT support, but only meet as often as your business requires it to avoid getting bogged down in IT details that should be handled day-to-day.
- Create a set of reports you can draw with the click of a button so that you can quickly review where you're at when you need to meet about something (like an Executive Summary). The reports need to include current software installed and licensing details, what your network health is (patch scores and so on), a basic hardware summary to spot potential problem machines, potentially unwanted applications and internet usage. It might sound like overkill for a small organisation, but this is where the problems creep in, so get your support provider to draw these up for you if you don't have the time.
- Have a budget planning session at least once a year. SMBs need to avoid cost surprises. Have this form part of a regular meeting cycle with your support provider. Include a clear view on risk factors for your business in this planning session to ensure you're covering the 'downside' of any cost savings.
- Review your support calls often as many costs come through not getting to the root cause of problems. If you're familiar with pivot tables in Excel, get some data in there and start analysing!

Questions you can ask your support company

- What am I currently getting from my IT and what is the roadmap for the next 12 to 24 months?
- What is the action plan to deal with disaster and failure?
- Is there a better or cheaper way to achieve my business goals through IT?
- How often do you review the support calls for my company?

What is an MSP and can they help?

Managed Service Providers (MSP) specialise in simplifying the day-to-day IT management of small to mid-sized businesses at a fixed and predictable monthly fee. A MSP uses specialized tools to monitor and manage your whole computer network and provide support either remotely or on-site along with various other services, specifically for companies with no or limited internal IT support. The key difference between an MSP and a regular computer support company is that the MSP benefits when their customers sites are running efficiently, whereas regular support companies make more money billing you for every hour they attend to your problems. That's a pretty compelling driver to create a true win-win partnership!