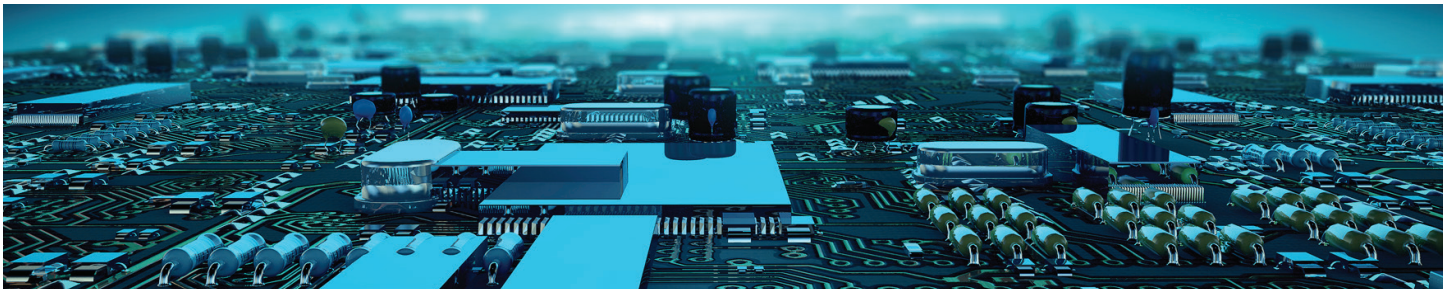


The Biggest IT Mistakes

Made by New *(and Not So New)* Small Businesses

by George Hefter, President
TCT Computer Solutions

For more information, or for help in any of the areas discussed in this paper, please give TCT Computer Solutions a call at (509) 627-4808, or send an email to info@tctcs.com. We'll be happy to help, and we look forward to the opportunity to become your technology partner.

PREAMBLE

In over 25 years of business we've seen just about every rookie mistake and poor choice that new (and not so new) small business owners make when setting up the IT infrastructure for their business. Usually, these choices and mistakes are made in the interest of saving money, which is understandable. However, if a business fails to appreciate just how critical a properly configured and functionally reliable IT infrastructure is to their success, these mistakes can end up costing them vast amounts of time and money in the long term.

All the individual pieces and parts that make up your IT infrastructure can affect how well your infrastructure functions, and thus can make, break, or needlessly complicate your business. If you are wondering what the heck an 'IT infrastructure' is, I am using that term to cover all the components that make up a business network, such as servers, workstations, network equipment, and all the cables. It also includes the software that makes the infrastructure work, the internet connection, and even the Internet Service Provider you choose.

Sound complicated? It is, and with so many component parts involved it is easy to see how ignoring or neglecting any area can quickly lead to problems. Nevertheless, small businesses routinely minimize or ignore many of these areas and settle for setting up a 'quick and dirty' network to support their business.

Let's discuss some of the most common problems we see every day in small businesses that call us for help.

TOP 6 IT MISTAKES BUSINESSES MAKE

1. Poor Quality Network Equipment

Most small businesses start out with a network composed of the same type of consumer-grade components that they use at home. But let's be real — your home network is typically used for browsing the internet, storing photos, doing homework, and maybe creating a few letters or updating your resume. Consumer grade equipment provides an adequate level of performance for these purposes. But it's typically not the end of the world if your home internet connection fails or doesn't work as well as you'd like.

Your business, on the other hand, provides your livelihood and therefore needs to work reliably all of the time. When it doesn't, you can find yourself unable to schedule service calls, invoice customers, record payments, or pay your employees. Let's face it – a disaster involving your business network can completely cripple your operation in a matter of seconds. This is why it's so important to ensure that it is set up correctly and uses quality components.

Business-class equipment is of higher quality and engineered to last longer in business use. It also typically offers more advanced features and better protection from threats than the consumer-grade products. When we see a typical home firewall/router, cheap switches, network cables running across the floor and through doorways, and an equipment room with no ventilation running at 120 degrees or more, it's not hard to figure out why the business might be experiencing network issues.

2. Poor Internet Connection

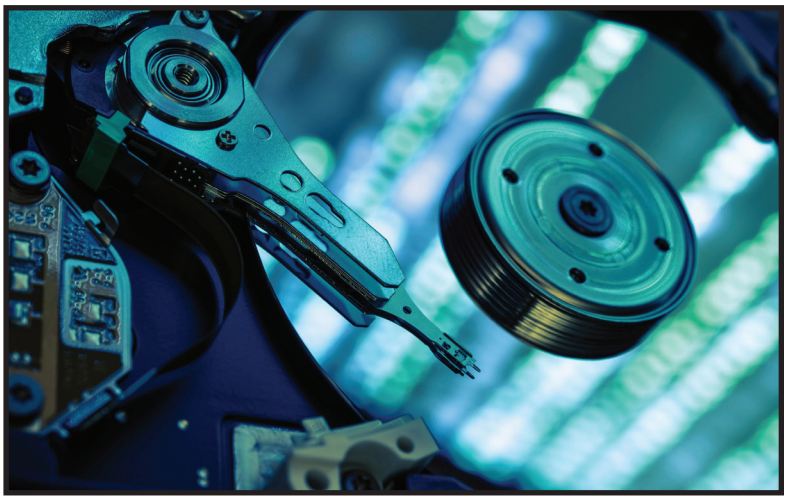
Most small businesses recognize the business need for an internet connection: email, invoicing, online payments, online banking...to name a few. So, they get an internet connection, often a very basic connection with limited bandwidth, only to find out later that the internet connection a business needs is quite different from an internet connection that satisfies most needs for a home user. A quick story from my own experience will make this point.

I was recently called to a small business having a problem with QuickBooks, a very widely-used business accounting package. To solve their problem, they chose to re-install the program from the original CD. That's fine, but they forgot that their version of QuickBooks was several years old and it has been updated many times since its original installation – 14 times, in fact. How do we get those updates? Well, the usual method is to download them from the QuickBooks website. Even though it turned out that I could get away with downloading only the most recent update, that download was very large and the customer's internet connection was a very slow, entry-level connection and it took well over two hours to download the required update. That customer paid for 2-1/2 hours of work for me to download and install an update that should have taken no more than 30 minutes with a better internet connection!

And that story illustrates only one aspect of the overall problem with a cheap but poor internet connection. Even if you spring for an internet connection with a faster download speed, which would have solved the problem in my story, what about upload speed? Internet connections that are 'asynchronous', i.e. they have faster download speeds but limited upload speed (like most cable and DSL connections), offer quick download speeds but make it difficult to upload large files like backups. That's often fine for home users where streaming music or movies is a principal use, but for many businesses the need to push large backup files out to the cloud or to an alternate location for disaster recovery requires a substantial upload speed as well.

Establishing two-way network communication between branch offices or between an owner's home and office will also require significant download AND upload speeds. Good internet connectivity in BOTH directions is an essential business need, not a luxury. The sooner you realize that, the better.

3. Outdated and Poorly Maintained Computers



Given that typical home computer usage is largely a mixture of internet browsing, online gaming, email, and homework, consumer-grade computers are manufactured and priced to be essentially throw-away products. With the increasing availability and use of smartphones for internet use and email, the pressure to make consumer-grade computers even less expensive further threatens the quality and durability of these products and makes them even less suitable for business use.

In addition, these machines are seldom (if at all) updated by their users with security and reliability patches, which makes them highly insecure and even less suitable for business use. But every day we are called to businesses where the computers are 10-year-old, dilapidated consumer-grade devices that haven't been upgraded in years. Many are still running Windows XP, an outdated operating system which is long past its official end-of-life and is no longer supported by Microsoft because its fundamental structure cannot be protected against today's security threats.

When we point out this problem to many small business owners, the common response is "We'll run over to Best Buy or Costco and pick up some new ones, and we'll have you set them up for us." It's clear they think this is a step in the right direction, but after we point out the weaknesses and shortcomings of consumer-grade products and the cost to make them truly business-ready, it becomes clear that business-class computers are the better option.

4. Inadequate or No Anti-Virus and Anti-Malware Software

With the headline-grabbing ransomware attacks that so frequently appear in the news, one would think that protecting your business from ransomware or other virus and malware attacks would get treated with some urgency. Sadly, this is often not the case. Putting the emphasis on price instead of actual security, it is very common to find that small businesses are using one of the many free endpoint security products that serve as come-ons for the more capable but higher-priced versions of those products.

While it's true that some virus protection is better than no virus protection, these free products are not, repeat NOT, adequate to protect a business from the ever-increasing onslaught of ransomware and malware programs. In fact, most of the paid versions also fall short of adequate protection in the face of newer and more malicious security threats that defy detection by any definition-based endpoint security products.

Current state-of-the-art endpoint security software is behavior-based and depends on detecting questionable activity rather than comparing downloaded code against thousands of code-snippets from known viruses. This behavior-based type of protection is far more likely to quickly catch and mitigate new viruses than the definition-based approach. Although more expensive, having best-of-breed endpoint security is far LESS expensive than the high cost of downtime, lost productivity, lost revenue, and possibly ransom that can cripple or end a business.

5. Unreliable or Inadequate Backup

Just one step up from no backup at all are infrequently performed and inadequately configured backups of important business software and data. We often see small businesses that back up their QuickBooks or other financial software to a flash drive or external hard drive that stays inserted into or attached to the associated computer and is infrequently, if at all, changed. This scenario is very risky for many reasons.

First, it provides no defense at all against a fire, flood, tornado, or any other natural disaster which could not only destroy the computer but the backup device as well. Second, if the device is attached to the computer when the computer gets hit by a ransomware virus, data on the backup device will be encrypted along with the data on the computer, eliminating any possibility of recovering without paying the ransom. And third, relying on only one backup device puts your entire backup protection at risk of failure of that one device. These devices DO fail, and often more frequently than most business owners might think.

So, what constitutes adequate backup protection? There are three principles that are essential for adequate backup protection: multiple devices, multiple locations, and multiple versions.

Multiple devices mean that whether you use flash drives or external hard drives, you should use more than one and change them every day. This will avoid the loss of ALL your backups in the event of a ransomware attack or device failure.

Multiple locations mean that at least one of the redundant backup devices not currently connected should be at one or more offsite locations. This prevents loss of all backups in the event of a break-in or natural disaster such as a fire or flood.

Multiple versions mean that multiple daily or even more frequent backups should be maintained to ensure that a damaged file can be restored even if many days (and many backups) have passed before the file damage is discovered. Nothing is more disappointing than discovering that a file, damaged two weeks ago but not accessed since then, cannot be recovered because all versions of the daily backup contain that same damaged file.

There are several ways to ensure that your backup regimen embraces all three of these principles. For example, multiple local devices like flash drives or external hard drives may be used with at least one device rotated offsite daily by an employee trusted to perform the rotation and offsite safekeeping. Or a high-capacity Network Attached Storage (NAS) device might be used for high-capacity, local storage of multiple backups along with the ability to replicate that storage to an offsite location or to cloud storage. In practice, this latter technique is far more reliable because once configured it does not depend on a conscientious human to operate reliably.

6. Failure to Recognize When a Domain and Server Should Be Used

We always shudder a little when we are asked to help a business that has as many as 20 or 30 workstations but it is still operating as a Workgroup or Homegroup. These network configurations are designed to allow small home or office networks of five or fewer computers to share internet connections and printers, but are ill-suited for larger, more complex networks. There are connection limits on such networks that quickly become problematic when more than five computers and several printers are in use. File access and network security are also greatly complicated in these networks and overall network management becomes a nightmare as these network configurations grow.

Once a network has grown to more than five users, consideration should be given to the use of a server and replacing the Workgroup or Homegroup configuration with a Domain configuration managed by the server. Access to shared files and shared resources like printers becomes far easier to manage, and user permissions can be set individually for each user in one location. Permissions can also be applied even for individual files, reducing the nightmare of convoluted folder permissions and other awkward user management issues brought on by the need for multiple user accounts to be maintained on each workstation.

Once your network gets larger than five computers, and certainly by the time it gets to 10 computers, you will need a local (or cloud) server and a domain to keep IT issues from taking up a large amount of time that could be better spent focused on the operation of your business.

BONUS: NOT NECESSARILY MISTAKES, BUT OFTEN OVERLOOKED SERVICES THAT ARE VERY USEFUL

Although not rightly characterized as 'mistakes', there are also several underutilized services that would highly benefit any small business and should be adopted early on. These are File Sharing and Collaboration, Hosted Exchange, and Hosted PBX (VOIP).

File Sharing and Collaboration

It may not be obvious, but most File Sharing and Collaboration tools like Intermedia's SecuriSync, eFolder's Anchor, DropBox, or OneDrive are cloud backup solutions as well. In addition to facilitating the transfer of large files to your accountant or lenders, allowing secure file access for selected offsite users, and enabling document collaboration for proposals and the like, these tools also maintain near real-time backups of the shared files. Some even maintain unlimited versions allowing rollback to essentially any point in time, a real plus for recovery from a ransomware attack or a corrupted file.

Hosted Exchange

Traditional email solutions utilizing POP or IMAP can be troublesome, especially when accessing the email account from multiple devices. Hosted Exchange solutions solve these problems and provide enterprise email features like shared calendars, public folders, and your own domain name for not much more than the typical cost of traditional ISP-based email. Most small businesses typically discover how useful these features are (or would be) not long after starting their business and interacting with customers and vendors who expect them.

Hosted PBX

Overlooked by most small business startups are the marketing and productivity value of a business class phone system. A 'hosted PBX' VOIP system leverages your internet connection and local network to economically provide enterprise-grade features like auto-attendant, hunt groups, call pickup, call queues, and 'find-me' call following at a fraction of the typically very significant cost of an on-premises phone system. Hosted PBX systems can even support branch offices or salesmen on the road. This usually takes a knowledgeable partner to set up, but also offers a 'must-have' productivity and image enhancement for a growing small business.

THE WRAP UP

This paper is by no means an exhaustive list of all the problems that we've encountered in 25 years of providing technology services to small and medium-sized business customers. But these problems are almost universal in their applicability to small and medium-size business startups, even for franchises when the franchise company doesn't provide the hardware and setup expertise. The advice offered in this paper, if followed, will go a long way towards ensuring that your business gets started on the right foot and continues to grow with the help of your technology and does not suffer because of it.

Check this list of frequent IT mistakes against your business operations and see if you make the grade. If not, please do not hesitate to call us for a free IT consultation.

509.627.4808