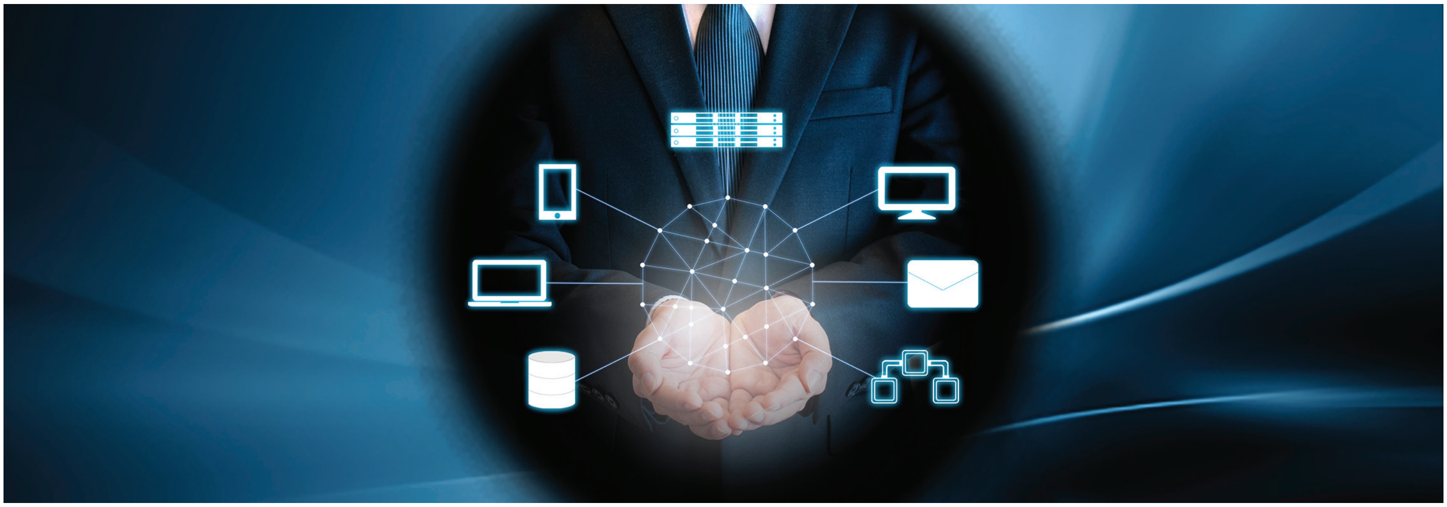

Why Your Business Needs Regular IT Support

Smart IT for Small Business

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

Convincing a small- or medium-sized business owner that their business needs regular IT support is one of the hardest challenges I've faced in over 25 years in business.

It was easier in the distant past when computers were less prevalent and required more arcane skills to operate. But in the nearly 50 years since the advent of the microcomputer in the late 1970s, these devices have rapidly become less costly and enormously easier to use.

It is difficult to find a household without at least one such device, and many people alive today have never known a time when they were not commonplace. This widespread familiarity with computers makes everyone believe they know why, when, and how to use a computer.

And thus, when someone decides to start a business, the notion of using computers as part of that business seems simple enough. That is a very big misconception for several reasons.

WHY YOUR BUSINESS NEEDS REGULAR IT SUPPORT

REASON 1:
A BUSINESS NETWORK IS VASTLY MORE COMPLICATED THAN A TYPICAL HOME NETWORK

Familiarity with a computer or even a small network at home does not usually mean that the business owner (or an employee) has the background, knowledge, and experience to set up and manage a reliable business network.

We encounter this problem almost every time we talk to a business owner about ongoing IT support. The business has usually called us in to help solve a problem that resulted from a lack of knowledge about the proper configuration of a business network, poor equipment choices, poor network security, incorrect workstation configuration, or some failure of their network server (if they even have one).

Many times, we find problems in all these areas. Even when we resolve the issue and explain that the problem was due to improper equipment or configuration, the owner typically resists the suggestion that ongoing support is needed.

The simple fact is that reliable business networking involves considerable knowledge about equipment choices, security issues, and networking configurations that rarely, if ever, are a concern for a home user. Without that knowledge, a do-it-yourselfer will make configuration errors, employees will tinker, new hardware will be incorrectly added to the network, security updates and backups will seldom be made, operating system and line-of-business updates will be overlooked, software or anti-virus subscriptions will expire, and problems of all sorts will continue.

A sad irony is that the more often an IT service provider is called to correct these issues, the more likely it is that the IT service provider will eventually be blamed for not correcting the problems. Because the business owner doesn't know what he doesn't know, he assumes that once corrected, a problem never re-occurs. But employees still tinker, software updates still occur, equipment gets added, new drivers become available, new threats emerge, and old problems come back or new problems result from the organic changes that inevitably occur in a business network. It takes a very long time before the fact sinks in that business networks need almost constant attention.

REASON 2:
THE CONSEQUENCES OF PROBLEMS CAN BE CATASTROPHIC

Many times, there is also a precipitating event such as a catastrophic equipment failure, or discovering after a ransomware attack that the last good backup was several months ago. These events just don't seem real to a business owner until they happen, and then the consequences in terms of protracted downtime and enormous recovery cost finally drive home the need for ongoing, professional IT support.

It can take weeks to order and receive a replacement server, and then several days more to configure the server and reload all the necessary software and data. Days of downtime can be crippling to a business; weeks could be disastrous.

Even without a catastrophic equipment failure, the consequences of virus or ransomware attacks can be almost as crippling. It can take days to fight off and clean up from a serious virus attack. It can take even longer to recover from a ransomware attack, even if you have good and current backups. If you don't have a good and current backup, your choices are to pay the ransom and hope you get the decryption key (assuming there is honor among thieves), or recover your data by hand from paper records. The former choice is likely to be both costly and time-consuming; the latter even more time-consuming and perhaps even more costly in terms of downtime. These events have crippled and even ruined businesses.

REASON 3:
POOR NETWORK PERFORMANCE AND DOWNTIME THREATENS BUSINESS SUCCESS

Thankfully, catastrophic events typically don't happen every day. But it doesn't take a catastrophic event to hurt the performance and profitability of your business. The most common complaints we receive from businesses without dedicated IT support have to do with the dozens of 'little' problems that take the business owner's time and attention away from actually running his business.

A poorly set up IT infrastructure can perform slowly or cause myriad problems with employee log ons, printing, internet access, point-of-sale performance, or any number of other annoying issues that get in the way of efficiency and productivity. A commonly encountered example is improperly configured DNS settings on a network server, which can make workstations 'take forever' to log on. While not a show stopper, this issue makes most employees wish they had stayed home that day.

Another common problem relates to the scheduling of periodic virus scans, which certainly need to be done but which typically and paradoxically usually default to 'at startup' or to some other equally inconvenient time during the day. Several anti-virus programs have a huge footprint which can impact performance even when a scan is not active, and they can slow a computer or an entire network to a crawl when the daily virus scan starts during business hours.

The same thing can happen when some types of backup programs are scheduled to run during working hours. 'File and folder' type backups should be scheduled to run during off hours because these backups frequently lock files while they are being backed up, creating sluggishness or errors if the files are in use. Backup frequency and scheduled run time(s) need to be carefully chosen.

These examples are only the ‘tip of the iceberg’ when it comes to subtle mistakes, forgotten steps, or well-meaning but clumsy tinkering that can affect network performance. Add to that:

- Poor equipment choices that do not have the required capacity or throughput.
- The all-too-common use of a second wireless router when an access point should be used.
- A mistaken sense of economy or conservation that prompts a decision to shut down equipment at the end of the day, making it impossible to run virus scans or backups after hours.
- Literally, dozens of arcane server or network configuration settings that can make all the difference between trouble-free use of the IT infrastructure and endless frustration over balky performance.

If you don’t think these things can and will happen, please refer to **“Reason 1:” on page 3**.

A poorly performing and improperly maintained IT infrastructure leads to frustrated employees, loss of productivity and efficiency, and a corresponding loss of revenue that can easily overshadow the cost of ongoing professional support.

REASON 4:
SMBs FREQUENTLY IGNORE COMPLIANCE REQUIREMENTS AND RISK HUGE PENALTIES

In this digital age, the proper handling and safeguarding of customer personal, financial, health, credit card, and other types of physical and electronic data is an obligation of every business, small or large.

Compliance requirements in most of these areas have been specified by the associated government agencies or professional organizations. Periodic audits are conducted to measure the adequacy and effectiveness of the regulations and the degree of compliance throughout the affected organizations.

Failure to adequately comply with the specified requirements can mean significant fines, enforced remediation, and, ultimately, loss of certification or license to perform the regulated functions or services. Some of the most common compliance requirements include:

- **PCI Compliance** – applies to any business that accepts credit card payments for its goods or services and designed to protect credit card and personal information.
- **HIPAA Compliance** – applies to health care providers of any size and designed to ensure both the safety and secure transportability of personal health information.
- **SOC 2 Compliance** – typically focuses on financial information security but can apply to any business that provides services requiring the handling of client business or customer information. SOC 2 is an auditing procedure that ensures your service providers securely manage your data to protect the interests of your organization and the privacy of your clients.
- **GDPR Compliance** – The General Data Protection Regulation was developed by the European Union (E.U.) to provide rules and standards related to privacy and data protection. If your U.S. organization does business in the E.U., offers goods and services to E.U. citizens, uses E.U. vendors, or processes E.U. citizen data, then all the provisions of GDPR may apply.

The list on the previous page is by no means all-inclusive. If you are a financial services company, you may also have SOX (Sarbanes – Oxley) compliance requirements to meet. If you do business with or provide services to city, state, or federal governments, there are a whole host of other regulations with compliance requirements. The list goes on and on and on.

In our experience with small and medium-sized businesses, a very large percentage of them pay only token attention to these or other applicable compliance requirements, if they pay any attention to them at all—until they are faced with an audit. Because many of these requirements deal with the security of electronic data, we then receive frantic phone calls asking if we can help and, occasionally, demanding that we come to their office 'right now' because the auditors are there or because the auditors have left them a rather lengthy questionnaire to complete.

What typically follows is the business's rather difficult and painful realization of two facts about compliance requirements: 1) they have expensive consequences for non-compliance and 2) they require significant process and procedure changes. Many of those process and procedure changes affect not only digital security steps such as firewall configuration and backups, but also internal process controls enforced by the business in its daily operations. Much of that latter work necessarily falls on the business staff, which does not usually come as welcome news.

While an IT service provider is not able to specify the internal procedural controls a business needs in much of its operations, an experienced IT service provider can not only specify and implement the necessary digital security steps but can also offer valuable insights about effective procedural compliance steps taken by its other clients with similar requirements.

An ongoing and trusting service relationship with your IT service provider will help ensure that you are ready for compliance audits, with little anxiety about the possible consequences.

SUMMING UP

The reasons for ongoing IT support presented in this paper are based on 26 years of experience providing continuous IT support to small- and medium-sized businesses of all types.

Look at any successful enterprise-level business you can think of and they all have an in-house IT support staff or dedicated IT support of some kind. Their IT infrastructure is the central nervous system of their enterprise; they understand that the success of their business depends on effective, reliable, and ongoing IT support. And even with that ongoing support, their IT-related failures sometimes make the news when some new threat takes them by surprise. But they are ready for such surprises and respond quickly. Could your business say the same?

The IT infrastructure of any small- or medium-sized business is no less important. Furthermore, effective and reliable IT support for such businesses does not require a costly in-house staff with all the associated payroll and benefits burdens. While the cost will vary somewhat depending on the size and complexity of the business and its related infrastructure, it will typically be no more than half the cost of the comparable in-house IT staff. For very small businesses, that will mean the services of an entire in-house IT department can be obtained for less than half the cost of an additional employee.

Don’t be lulled into thinking that what you or an employee knows about home computers or on-line gaming has given you the knowledge and experience to effectively manage your business network. With extremely rare exception, you don’t! And this paper presents some key reasons for that bold statement.

Don’t you have enough to do to ensure your *ENTIRE* business runs well? A smart manager doesn’t do everything—he or she coordinates the efforts of others who have the right skills for the task. Get on-going IT support from a reliable and experienced company with a good reputation and focus your efforts on running your business. You won’t be sorry.

Please do not hesitate to call us for a free IT consultation.

509.627.4808