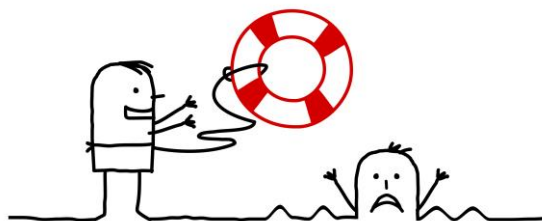


# THE PRACTICE ADMINISTRATOR'S GUIDE

For Finding A Professional, Competent, Honest, On-Time,  
Fairly Priced & Dependable  
IT Service Company



By: Chuck Poole

**First Edition**

Read this book and you'll discover:

- ✓ The five types of technical support available, and the pros and cons of each.
- ✓ Five critical facts you must know before moving to the cloud.
- ✓ How to avoid getting ripped off, disappointed, and/or paying for substandard work.
- ✓ 12 warning signs that you hired the wrong IT service company.
- ✓ Viruses, worms, spyware and hackers: what you need to know to protect your firm from invasion.
- ✓ Everything you need to know about contracts, payment schedules, and rate negotiations.
- ✓ 21 revealing questions you should ask any IT service company before giving them access to your firm's network.
- ✓ Why you should avoid "cheap" or "bargain" computer repair shops.
- ✓ How to turn technology into a competitive advantage instead of a drain on your time, money, and resources.
- ✓ What are "managed services", and why your firm needs managed services?

All rights reserved. No part of this publication may be reproduced or transmitted in any form by any means, electronic or mechanical, including photography, recording or information retrieval system, without written permission from the author.

Printed in the USA.

Copyright © 2013 Technology Marketing Toolkit, Inc. and PalmTech.

# CONTENTS

|  |    |
|--|----|
| Preface.....   | 1  |
| Introduction .....   | 3  |
| Business Is Becoming (Technically) More Complicated  | 3  |
| Downside Of Technology   | 3  |
| Computer Consultant Horror Stories   | 4  |
| What This Book Will Teach You  | 6  |
| Chapter ONE.....   | 8  |
| The True Cost of Downtime  | 8  |
| The Cost Of Bad Advice   | 10 |
| Chapter TWO.....   | 12 |
| What Are Your Options for Technical Support?   | 13 |
| Chapter THREE.....   | 22 |
| Secrets to Choosing a Great IT Service Company: What to Look For, What to Avoid, What to Demand! | 22 |
| The 4 Most Costly Misconceptions About IT Service  | 23 |
| 21 Questions You Should Ask Your IT Service Company Before Hiring Them To Support Your Network   | 28 |
| 12 Warning Signs that You Hired the Wrong IT Service Company                                     | 37 |
| 4 Mistakes To Avoid When Choosing An IT Service Company  | 38 |
| Chapter FOUR.....  | 41 |
| Avoiding Project Nightmares, Disasters, and Expensive Miscommunications                          | 41 |
| Determine Your Priorities  | 42 |
| A Quick Word on Price  | 43 |
| Start Small  | 43 |
| Demand A Fixed Price   | 43 |
| Get Everything In Writing  | 44 |
| Do Your Research   | 44 |
| Communicate Your Concerns  | 45 |
| Chapter FIVE.....  | 46 |
| How to Get the Most Out of Your IT Service Company   | 46 |
| Take Responsibility For Your Own Protection  | 46 |
| Keep Spyware, Malware, And Viruses Off Your Network  | 48 |
| Be Aware Of Sneaky Ways Hackers Invade Your Network  | 49 |
| Create And Enforce An Acceptable-Use Policy (AUP)  | 50 |
| Allow Your Consultant To Maintain Your Network   | 50 |
| Be A Great Client  | 52 |

|  |           |
|--|-----------|
| Six Ways A Good Relationship With A Competent IT Service Company Benefits Your Firm                    | 53        |
| <b>Chapter SIX.....</b>  | <b>54</b> |
| Preventing Network Disasters with Proactive Maintenance  | 55        |
| How Managed Services Can Prevent These Disasters From Happening To Your Business                       | 55        |
| What Are The Benefits Of Managed Services?   | 56        |
| What To Look For In A Managed-Service Plan   | 58        |
| <b>Chapter SEVEN.....</b>  | <b>62</b> |
| Moving To The Cloud  | 62        |
| 5 Critical Facts You Must Know Before Moving To The Cloud  | 62        |
| What Is Cloud Computing?   | 63        |
| What About Office 365 And Google Apps?   | 65        |
| Pros And Cons Of Moving To The Cloud   | 65        |
| Different Types Of Cloud Solutions Explained:  | 68        |
| FAQs About Security, Where Your Data Is Held, And Internet Connectivity                                | 69        |
| What To Look For When Hiring A Cloud Integrator  | 71        |
| 5 Critical Questions To Ask Your IT Service Company BEFORE Letting Them Move Your Network To The Cloud | 72        |
| <b>Chapter EIGHT.....</b>  | <b>74</b> |
| Contracts, Payment, Schedules, and Rate Negotiations   | 74        |
| Warranties, Guarantees, And Making Things Right  | 74        |
| Payment Terms  | 75        |
| Project Timeline And Completion Date   | 75        |
| Changes, Modifications, And “Scope Creep”  | 76        |
| Hardware, Software, And Materials  | 77        |
| Hours And Conditions Of Work   | 77        |
| <b>STAY SECURE.....</b>  | <b>80</b> |
| Computer Security  | 80        |
| Network Security   | 81        |
| Email Security   | 81        |
| Internet Security  | 81        |
| Mobile Security  | 82        |
| <b>I.T. Dictionary.....</b>  | <b>83</b> |
| Technical Terms Explained in Plain English   | 83        |
| <b>An Invitation to the Reader.....</b>  | <b>88</b> |





# *Preface*

My entire life has been devoted to the passionate pursuit of Computer Technology. At age 10 I helped build my first computer from a mail order kit because at that time you couldn't buy a desktop computer in any store – anywhere. (Yes, I admit this was a LONG time ago). That same year I was learning to write functional programs to solve simplistic business problems and teaching curious adults how to use and program them. By age 18, I was one of a handful of experts in the country that could write a specialized form of telecommunication software that could intercept and route phone calls internationally. I had software contracts with the FBI, CIA, United Nations, and had deployed software in more than 38 countries for various National telecommunication authorities. Some of these software systems are still being used 20 years later. As a software designer and developer, I had to work closely with a variety of different clients who all basically wanted the same thing: elegant solutions that were easy to learn, solved core business problems, and were cost effective to modify and maintain. Throughout my career I watched the computer industry grow, thrive, and become much more integrated with the needs of business. The only problem was that somewhere along the line “computer people” decided that more complicated systems were always better. I'm not sure why this came to be, but it's great to see new ideas are starting to win the hearts and minds of the marketplace. The iPhone was the first computing device that went “backwards” in design and proved that simplicity can be highly rewarded. When I sold my software development business in 2003, I decided that I would tackle many of the wrongs that I saw in the Computer Consulting community. Whether it was a salesperson trying to convince a client that they needed the latest and greatest superfluous computer gadgets, or an IT consultant who just couldn't get the job done, most IT service companies simply didn't live up to their clients' expectations.

When I started PalmTech more than a decade ago, I instantly realized that most of our potential clients didn't care how their technology functioned, as long as it “just worked” and allowed them to

be good at what they do. It is with this mindset we start each day: to organize, standardize, simplify, react swiftly to issues, and ultimately boost productivity. Our belief is that if your Information Technology is not helping you increase your profits, it's not being implemented correctly. I hope you find this book useful in your pursuit of a better solution for your firm or business.



# *Introduction*

## **Business Is Becoming (Technically) More Complicated**

There is a powerful force driving all businesses to deliver superior products and services faster and on tighter margins—technology.

Every business, from small mom-and-pop stores to large enterprises, relies on technology. Whether it's e-mail, e-commerce, websites, cloud computing, database management, or accounting software, there are very few businesses that don't have some level of dependence on their computer network and the various applications and data it stores.

The upside of technological advances is tremendous. When applied correctly, technology can provide your business with significant competitive advantages in greater profitability, increased productivity, improved customer service, and up-to-the-minute reporting for strategic planning and decision making.

## **Downside of Technology**

The downside of this dependence on technology is that when it doesn't work it can become a tremendous source of frustration, putting a major strain on production, sales, fulfillment, and eventually...profit. No business is immune from computer problems and failures. Without proper network maintenance, the average business can end up with spyware, viruses, and system crashes that can easily turn into major network outages. And that's not including the daily computer "glitches" and problems that frustrate you and your employees.

Then there's the complexity of it all. Installing and supporting even a small network requires specialized knowledge and skills that most firm administrators don't have in-house, and the margin for error is greatly reduced in a small business. If a large corporation makes a \$50,000 technology mistake, it's certainly not a good thing, but it only represents a minor blip in their overall IT budget. If a small business makes a \$20,000, or even a \$10,000, technology mistake, it significantly impacts their profitability and cash flow!

If you're like most firm administrators, you probably shy away from things technical in nature because you don't understand how they work, why they work, or how to operate them. After all, what you want are business solutions to drive revenue and profitability, not the latest and greatest gadgets and budget-busting nonsolutions that break and make your life more complicated. Yet the technology that runs your business is too important and too expensive to ignore.

- ✓ So how do you make sure that the hardware, software, and solutions you are investing in actually support your business goals and work the way they are supposed to?
- ✓ How do you stay on top of technological advances that will give you significant competitive advantages while steering clear of the "latest and greatest" fads?
- ✓ How do you make sure your data is protected from an ever-growing list of threats, including viruses, hackers, spyware, faulty hardware and software, and even employee sabotage?
- ✓ And ultimately, how do you go about finding a reliable IT service company that not only has the expertise to make all of this technology work for you, but also the business acumen to recommend and implement real solutions that enhance productivity and profitability?

That's what this book is about: arming you with the basic information you need to find a trusted advisor who can help your small business tame technology and turn it into a powerful, competitive weapon instead of a huge financial strain and source of problems.

## **Computer Consultant Horror Stories**

Unfortunately, there is no shortage of horror stories about unbelievably bad customer service from IT service companies and computer consultants. They range from annoying computer technicians who take forever to return a phone call to horror stories about fly-by-night computer repair shops or consultants who delete all the data

stored on a network as a result of their unethical or incompetent behavior. If you talk with your own friends and colleagues, I'm sure you'll get an earful of the unfortunate experiences they have encountered in this area.

The biggest reason for this is that the computer services industry is not regulated like many other industries. Almost anyone who can turn on a computer can set up a computer repair shop, regardless of his actual knowledge and expertise. Compare this to automotive repair shops, electricians, plumbers, lawyers, realtors, dentists, doctors, and accountants (to name a few) who are heavily regulated to protect the consumer from receiving substandard work or getting ripped off. However, because the computer industry is still very new, there aren't many laws in existence to protect the consumer.

The upside is that most IT service companies are ethical and will not try to cheat you or take advantage of you. But unethical IT service companies aren't the biggest problem—*incompetent* IT service companies are. Even if they are honestly trying to do a good job, their inexperience can cost you dearly in inflated support bills, poor network performance, lack of security, and data loss.

That is where this book will come in handy. It gives you basic, need-to-know facts to help you find an honest, competent IT service company who can contribute to your business's success. By arming more firm administrators with this information, I am hoping to raise the standards within the IT service industry, and to give you, the consumer, information to help you guard against the unethical conduct or incompetence of some companies and consultants.

**Note:** While there are plenty of women in the IT service industry, the large majority are men. For simplicity, I will therefore refer to computer consultants in the masculine gender throughout this book. You will also notice that I sometimes use the term “computer consultant,” “computer consulting company,” “computer Service Company,” “IT Service Company,” and sometimes the word “technician.” All of these terms refer to the person or company providing advice, products, services, and support for your computer network. However, “consultant” is usually used to define someone with

a higher level of expertise and knowledge, whereas “technician” connotes someone who simply knows how to fix computers.

## **What This Book Will Teach You**

- How to become an educated buyer of IT support and services.
- How to avoid getting ripped off by an incompetent, unethical IT service company.
- How to reduce your IT costs.
- How to secure your network and data from viruses, spyware, hackers, loss, natural disasters, and disgruntled employees.
- How to reduce or eliminate computer problems and headaches that frustrate you and waste your time.
- How to turn technology into a competitive advantage instead of a drain on your time, money, and resources.



# Chapter ONE

## The True Cost of Downtime

Every business, large or small, depends on technology at some level to operate. If you've owned a computer for more than five minutes, you know that no one is exempt from computer problems, system crashes, and downtime. While all firm administrators can relate to the sheer frustration these issues create, few can put a dollar figure to the actual hard cost to their business. That is because so much of it is soft costs related to productivity, hours worked, and time lost.

What makes the cost of computer downtime even more difficult to determine is the fact that no business is "average," and therefore statistics that quantify the cost of downtime for the average company are worthless.

However, no business owner can deny that an interruption in their business costs them money, whether that interruption is caused by a server crash, hardware failure, or some other outside force. If you've ever had your business grind to a screeching halt because you and your employees could not access the data or systems necessary for operations, you must have some idea of the frustration and financial loss to your business, even if you didn't put a pencil to figuring out the exact dollar amount.

Take a look at these statistics:

- Companies experience an average of 501 hours of network downtime every year, and the overall downtime costs an average of 3.6% of annual revenue. (*Source: The Costs of Enterprise Downtime, Infonetics Research*)
- 93% of companies that lost their data center for 10 days or more due to a disaster filed for bankruptcy within one year of the disaster, and 50% filed for bankruptcy immediately. (*Source: National Archives & Records Administration in Washington*)

- 20% of small to medium businesses will suffer a major disaster causing loss of critical data every 5 years. (*Source: Richmond House Group*)
- Last year, 40% of small to medium businesses that manage their own network and use the Internet for more than e-mail had their network accessed by a hacker, and more than 50% didn't even know they were attacked. (*Source: Gartner Group*)
- Of those companies participating in the Contingency Planning & Management Cost of Downtime Survey, 46% said each hour of downtime would cost their companies up to \$50,000; 28% said each hour would cost between \$51,000 and \$250,000; 18% said each hour would cost between \$251,000 and \$1 million; and 8% said it would cost their companies more than \$1 million per hour. (*Source: Cost of Downtime Survey Results, 2001*)
- Cybercriminals stole an average of \$900 from each of 3 million Americans in the past year, and that doesn't include the hundreds of thousands of PCs rendered useless by spyware. (*Source: Gartner Group*)

But even if you don't factor in the soft costs of lost productivity, there is a hard cost of repairing and restoring your network. Most major network repairs will require an average of 4-8 hours to get the network back up and running. Plus, most consultants can't get on-site to resolve the problem for 24 to 48 hours. That means your network could be down for one to two days.

Since computer consultants often charge over \$100 per hour, plus a trip fee and a surcharge if it's an emergency, the average cost of these repairs is \$600-\$1,000. Over a year, this results in \$1,800-\$3,000 in costs, not including hardware and software or lost sales and work hours. Of course, those numbers quickly multiply with larger, more complex networks.

## The Cost of Bad Advice

In addition to downtime, there is another expense that most firm administrators don't consider: the cost of bad advice when an inexperienced consultant recommends a product, service, or project that is unnecessary or incorrect for the business owner's specific situation.

Another form of bad advice is when an IT service company doesn't take into consideration all the pitfalls and situations that will arise when implementing your project, and grossly underestimates the time and money it will take to successfully complete it. When this mistake is made, your project ends up way over schedule, and it costs you 2-3 times as much in unexpected fees, hardware, and software.

It's gotten so bad that *Network World* recently noted, "Increasingly, IT customers are crying malpractice and railing against slipped implementation schedules, compounded consulting fees, and disappointing product performance."

Although the price of bad advice is hard to measure, if you've ever been disappointed or burned by a so-called IT expert, you know the costs to your business are painfully high.

Here are just a few of the ways bad IT advice can cost you:

- Paying for unnecessary projects, software, or hardware.
- Paying too much for repairs, software, and hardware.
- Accumulating downtime, unstable networks, data loss, and security breaches.
- Getting stuck with a "solution" that doesn't really solve your problems.
- Increasing the time and work you and your employees invest in rolling out a project.
- Paying double by having a competent service company fix what the first company/person messed up or complete the project you originally wanted implemented.



- Incurring litigation costs to get your money back from a company or technician who ripped you off.
- Dealing with the sheer frustration of the problems resulting from poor advice.

Trouble is, it's hard to know that you're paying for bad advice until you are already neck-deep into the problems. By the time you get the first inkling that you hired the wrong company, you've already invested a considerable amount of time and money, making it difficult, if not impossible, to end the project and look for someone else. That's why the information in this book is so critical. Your best defense against all this heartache is to become an educated consumer who does your homework.



# **Chapter TWO**

## **What Are Your Options for Technical Support?**

With the constant changes to technology and the daily development of new threats, even a small network requires ongoing maintenance from highly-trained consultants to ward off viruses, spam, spyware, slowness, user errors, and data loss. However, hiring a full-time IT person is not always feasible for small to medium businesses. In fact, to support most medium business networks, a competent desktop technician, server engineer, and network engineer may be needed. If your business can't justify hiring a full-time employee (or possibly three full-time employees), you only have three options for computer support:

### **Option #1: Don't do anything.**

This is sounds crazy, but we see it every day: businesses that don't pay attention to the care and maintenance of their network until it stops working. Then they are forced to call in an expert to repair or replace whatever caused the problem.

This reactive model of network support is similar to ignoring oil and filter changes in your car until smoke starts pouring out from under the hood. Taking a reactive approach to network maintenance is a surefire path to extensive downtime, lost data, and excessive spending on IT support, not to mention major disruptions in staff productivity, sales, production, and customer service. Even if your computer network appears to be working fine, there are a number of daily, weekly, and monthly maintenance tasks that must be performed to keep your data secure and your systems running smoothly. A short list of these tasks includes:

- Virus scans and updates
- Security patches and updates
- System backups and disaster-recovery planning
- Spyware detection and removal
- Server and desktop optimization

- Mobile device management
- Employee policies and monitoring
- Intrusion detection
- Spam filtering

If you run specialized practice-management, customer-relationship management, or production software, or if you have multiple locations, a wireless network, highly sensitive data (as in financial or medical organizations), or other specialized needs, the list will get even longer. Remember, your computer network is just like your car or your house. They all need regular maintenance to avoid problems.

If you learn only one lesson from this book, I hope it will be to proactively monitor, maintain, and secure your network instead of choosing to react to network and computer problems as they arise. Aside from a telephone, your computer network and the data on it are undoubtedly the most important business tools in your office. When they are unavailable, all productive work comes to a grinding halt.

As the old saying goes, an ounce of prevention is worth a pound of cure; this goes double for your computer network. Unfortunately, most firm administrators are under the incorrect assumption that regular computer maintenance isn't necessary, and therefore only call in an experienced IT service company when something goes wrong. As stated previously, this model of "break-fix" computer support is not a good idea, especially if the operation of your network and the data on it are important to your business.

## **Option #2: Do it yourself.**

Although this option is better than doing nothing, it still puts you at risk for computer network disasters. Instead of hiring a qualified service company to support your network, you designate the most technically-knowledgeable person on staff to be your makeshift IT manager, and bring in outside help only when you run into a network crisis you can't solve.

Problem is, you are pulling these people away from the real job you hired them to do, and unless they have the time to stay up-to-date on the latest developments in IT support, security, and management, they don't have the skills or time required to properly maintain and secure your network and could actually worsen the situation. This inevitably results in a network that is ill-maintained and unstable, which may cause excessive downtime, overspending on IT support, and expensive recovery costs.

Another variation of this option is to get your neighbor's kid or a friend to provide computer support on a part-time basis. This is a mistake for two reasons: First, they may not be fully qualified to handle the job, so they could make things worse. They may be able to fix the problem in the short-term, but they might not have the time or expertise to get to the root of the matter. Second, they may not always be available when you need them. If your server goes down at 9:00 AM, they might not be able to come until later that day or evening, or next week, causing you to lose a full day or more of productivity.

Also, as mentioned previously, they are providing reactive support. As with all things in life and business, it is far less expensive to prevent problems than to clean them up. If your part-time technician is not performing regular maintenance and monitoring of your network, you are susceptible to more problems.

### **Option #3: Outsource your support to a competent IT service company.**

Obviously, this is going to be the fastest and surest way to solve your computer problems. However, there are an ever-growing number of companies springing up across the country that offer computer repair services and support, which makes it difficult for a business owner to know which vendor is right for them.

As it stands today, there are five types of external computer support you can use:

## **1. Vendor support:**

Phone support provided by Dell, HP, Microsoft, AT&T or any of the big software and hardware vendors. If you've ever tried to get technical support from a large manufacturer or store, you know how frustrating it can be.

First, many vendors don't provide free support. If they do, it is usually very limited and only available by e-mail or Web response forms. If you are lucky enough to reach the support department, you'll end up going through a maze of phone options before you get a live person, and then the person is usually a nontechnical customer service representative who can't provide any real assistance. In most cases, they'll be located in another country, and may even be difficult to understand (many technology companies outsource their customer service because it's cheaper than employing U.S. workers). You'll also get a different person every time you call, and most will not have any particular knowledge about your business or what you are trying to achieve.

Here's another problem with vendor support: They aren't going to help you solve problems that aren't related directly to their hardware or software. For example, let's suppose you're having trouble connecting to the Internet, so you call your local provider. If their service is not causing the problem, you're stuck. Maybe your firewall is not configured right. Maybe the cable is not connected properly. If your problem is even partially related to another software or piece of hardware on your system, they won't help you.

## **2. Computer support hotline services:**

These services work like prepaid calling cards. For a set fee, you'll get an 800 number to call for 24-7 technical support. Sounds reasonable, but it's not all it's cracked up to be.

If you are a home user with simple application problems and questions, this service may work well for you. However, if you

are a business with mission-critical data, the last thing you want is a junior technician giving you advice. Also, some problems simply need to be analyzed on-site. Finally, these services are set up to deliver basic computer support, not to troubleshoot server problems, help with data recovery, or provide proactive maintenance.

### **3. The part-time technician just getting started:**

This is usually someone who left a job in the IT department of a company, got fired, or lost a job due to downsizing. Either way, he decided to start his own business with the dream of making lots of money by providing computer support to small businesses.

In many cases, he will try to do a good job for you. He means well, will often work cheap, and is usually eager to please. He might even have been referred to you by a friend or business colleague.

Although he has every intention of providing you with good service, there are some things you need to consider before hiring him to work on your network. Since most of these folks work from home, they don't have a secretary or office staff to handle your requests. When you call, you'll either get:

- An answering machine.
- A spouse, friend, or child who will take a message (which might or might not reach the technician).
- No answer and no voice mail; the phone just keeps ringing.
- The technician on his cell phone. Unfortunately, he's usually at another client's site, in his car, or taking care of some personal business (you catch him at the doctor's office or in a noisy restaurant).

The problem with this choice is response time; if you have a major network crisis, you need to know that you can get in touch with your consultant AND get a call back or response immediately. But it doesn't end there ...

Another problem you'll encounter is availability; the technician might not always be around when you need him. What happens if he leaves town for a week or has to go to the hospital? Or two or more of his clients experience a major emergency at the same time? Or the going gets tough and he decides to take another job? These are all scenarios that happen frequently with computer technicians who haven't established best practices and systems in their businesses. And if he is only supporting your network part-time, you can bet your emergency is going to take a back seat to his full-time employer.

Guaranteeing his work is another problem for the part-timer. Most don't have a professional contract, proposal, or invoice to give you, which means you have no written paperwork or contractual agreements to fall back on if things go wrong. Plus, most don't carry insurance, and can't compensate you if they accidentally screw up your network or cause you to lose data.

Even if he guarantees his work, how do you know he'll be around to fulfill his promises? Addresses and phone numbers can be changed instantly, and your one-man-wonder can disappear, leaving you no recourse or recovery.

Another player that we'll add to this category is the local business-machine companies. While they've created successful businesses selling fax machines and copiers, many have decided to start offering a full range of IT services. The problem is that they usually use their copier-technicians or hire junior computer technicians who know very little about desktops, laptops, servers, and networks.



#### **4. The “major player” tech-support company:**

This vendor is the complete opposite of the one-man-band. They may have multiple technicians, multiple locations, and a support crew. They might even have locations across the country. There are many first-rate IT service companies in this category that can be trusted to do a good job for you. As a matter of fact, many have the staff and resources to do an outstanding job.

So what’s the problem? Their schedule, price, and availability! In many cases, these companies are so busy servicing a number of large, profitable clients that they might not give a new client the service, response time, and support they need. They also may charge you exorbitant fees to cover their massive overhead of staff and offices. If you own a big business, with a big IT budget, you’ll do just fine with this type of company. However, if you own a small or medium business with a conservative IT budget, this may not be the best option for you.

Since you don’t represent a large windfall of profits for them, big tech-support companies may delegate their junior technicians, who are just learning the ropes, to support your network, saving the experienced consultants for their more profitable clients. As a business owner yourself, you can hardly blame them for taking this approach but, as a customer, you don’t want to be the small fish who is easily brushed aside.

Just like the big vendors, the larger the tech-support companies get, the less personalized the service becomes. You may not always get the same level consultant working on your network, and you might not be able to talk directly with a consultant when you truly need one. Being part of a large franchise doesn’t guarantee great service either; it just means they were able to write a check to cover the franchise costs. That doesn’t automatically buy them good business sense, technical skills, and/or customer-focused service.

## **5. An independently-owned computer consulting firm:**

You might accuse me of being biased here, but please give me a minute to explain my position before you dismiss my advice.

First of all, I've been doing business in this industry for many years, so I have considerable experience working with, and talking to, hundreds of other IT service companies. I've seen the horror stories and heard the complaints firm administrators have with all technology service vendors. Based on that experience, I think the best option for a small business is an independent consulting firm that is locally owned and operated.

The business you choose to support your network should be large enough to provide back-up support and fast response times, but small enough to provide personal service. That is the way we've modeled our company, and we've been able to deliver consistent, professional services.

We certainly don't feel as though our model is the sole option you can choose, and the size of a company is certainly not the only way to know in advance how professional and competent they will be. There are firms in all the choices outlined above that may do a great job for you.

The remainder of this book will further outline what to look for when choosing an IT service company for your business.



# **Chapter THREE**

## **Secrets to Choosing a Great IT Service Company: What to Look For, What to Avoid, What to Demand!**

Choosing an IT service company isn't easy. There are no shortages of horror stories about incompetent computer repair "gurus" bungling jobs and causing MORE problems as a result of their loose morals or gross incompetence. I'm sure if you talk to your own friends and colleagues you will get an ear-full of the unfortunate experiences they have encountered in this area.

Why is this? Because the computer repair and consulting industry, along with a lot of other industries, has its own share of incompetent or unethical businesses who will try to take advantage of trusting firm administrators who simply do not have the ability to determine whether or not they know what they are doing. Sometimes this is out of greed for your money; but more often it's simply because they don't have the skills and competency to do the job right, but won't tell you that up front. From misleading information, unqualified technicians, poor management, and terrible customer service, we've seen it all...and we know they exist in abundance because we have had a number of customers come to us to clean up the disasters they have caused.

### **Buyer Beware: The IT Service Industry Is NOT Regulated**

Here's an embarrassing (and little-known) fact about my industry: it is not regulated like many other professional service industries which means ANYONE can claim they are a "technology expert." In fact, a lot of the businesses in this industry started because the owner was fired or laid off from their job and couldn't find work anywhere else.

Automotive repair shops, electricians, plumbers, lawyers, realtors, dentists, doctors, accountants, etc. are all heavily regulated to protect the consumer from receiving substandard work or getting ripped off. However, the computer industry is still highly unregulated, and there aren't many laws in existence to protect the consumer – which is why

it's so important for you to arm yourself with the information contained in this book.

Anyone who can hang out a shingle can promote themselves as a computer expert. Even if they are honestly trying to do a good job for you, their inexperience can cost you dearly in your network's speed and performance or in lost or corrupt data files.

## **The 4 Most Costly Misconceptions about IT Service**

### **Misconception #1: My computer network doesn't need regular monitoring and maintenance.**

This is probably one of the biggest and most costly misconceptions that firm administrators have. Usually this is because they've been fortunate enough to never have encountered a major disaster; but that's similar to someone thinking they don't need to wear a seat belt when driving a car because they've never had an accident.

Computer networks are complex and dynamic systems that need regular updates and maintenance to stay up, running fast and problem free. In fact, it's surprising how fast a brand-new PC will slow down after a few weeks of use without proper updates and maintenance. Here are just a FEW of the critical updates that need to be done on a weekly – if not daily – basis:

- Security patches applied – with NEW viruses and hacker attacks cropping up DAILY, this is a CRITICAL part of maintaining your network.
- Antivirus updates and monitoring
- Firewall updates and monitoring
- Backup monitoring and test restores

- Spam filter installation and updates
- Spyware detection and removal
- Monitoring disk space on workstations and servers
- Monitoring hardware for signs of failure
- Optimizing systems for maximum speed

Just like a car, if you don't change the oil, replace the filter, rotate the tires, flush the transmission, and perform other regular maintenance on your car, it will eventually break down and cost you FAR MORE to repair than the cost of the basic maintenance – and cars are far simpler than a computer network!

**If your computer support tech does not insist on some type of regular, automated monitoring or maintenance of your network, then DO NOT HIRE THEM.** Lack of system maintenance is the NUMBER ONE reason most people end up losing valuable files and incurring heavy computer support bills. If your technician isn't offering you these services, you need to find someone else to support your computer or network for two reasons:

1. Either they don't know enough to make this recommendation, which is a sure sign they are horribly inexperienced, OR
2. They recognize that they are *profiting* from your computer problems and don't want to recommend steps towards preventing you from needing their help on an ongoing basis. After all, they'll get paid MORE to remove a virus than to make sure your system is patched, updated, and secured (which can be done quickly and inexpensively with good monitoring).

Either reason is a good one to get as far away from that person as possible!

## **Misconception #2: My nephew/neighbor's kid/brother-in-law/office manager knows this computer stuff and can take care of our computers.**

Most people look for a part time “guru” for one reason: to save a few bucks; but this often comes back to haunt them. We frequently get calls from firm administrators who desperately need our help to get them back up and running or to clean up a mess that was caused by an inexperienced neighbor, friend, or relative who was just trying to help.

If the person you have working on your machine does not do IT service/support for a living, there is a good chance they won't have the knowledge or experience to truly help you – they are a hobbyist at best. And do you really want a part-time, inexperienced person responsible for handling something as important as your data and computer network? As with everything in life, you get what you pay for. That's not to say you need to go broke to find a great technician, but you shouldn't be choosing someone on price alone.

## **Misconception #3: All IT service companies are created equal. Your best option will be the one who offers the lowest price.**

As I stated a moment ago, you get what you pay for. A cheap price usually means a cheap job. Really good technicians do NOT work cheap because they are in high demand just like every other professional service category. The only technicians that will work cheap are those that are just starting, and they are often-times grossly inexperienced.

And some shops will hire college kids or newbie technicians because they will work for next to nothing to gain experience, OR they allow interns to support your network because they don't have to pay them at all – but what you don't realize is than an inexperienced technician like this can end up costing more because:

1. They improperly diagnose problems, which means you're paying them to fix the **WRONG** thing and they **STILL** won't resolve your problem. Case in point: A few years ago a TV reporter went undercover to eight computer repair shops in Los Angeles, California with a perfectly working PC, but simply disconnected a cable in the back (a fix that the **AVERAGE** computer technician would have caught in minutes with a visual inspection). Several shops improperly diagnosed the problem and wanted to charge them anywhere from \$59 to over \$275 to fix it!
2. They could take 3 to 5 times as long to do the same repair as an experienced technician could fix quickly. Again, you're paying for those extra hours.
3. They could do **MORE** damage, costing you more money and downtime.

With your client data, accounting records, e-mail, and other critical data at stake, do you **REALLY** want the lowest-priced shop working on your machine?

We take the view that most people want value for their money and simply want the job done right. In my own business, I decided a long time ago that I would rather explain our higher rates **ONE TIME** than to make excuses for **POOR SERVICE** forever.

#### **Misconception #4: An honest IT service company should be able to give you a quote over the phone.**

I wish this were true, but it usually isn't. Just like a good doctor, an honest and professional technician will need to diagnose your network before they can quote any price over the phone; consider the example above where all that was needed was a simple cable being plugged in. If someone brought that to us, we would just plug it back in and not charge them; but without **SEEING** the machine, we could have never diagnosed the problem over the phone.



Also, some consultants will quote you a cheap rate over the phone to get in the door, but then increase the prices once they get in your office by taking three times as long, selling you add-ons and up-sells, etc. And finally, reputable firms don't charge by the hour anyway -- they give you a fixed, flat rate. Here's why...

One of the easiest ways to take advantage of a customer is to get them to agree to a time and materials repair. Unless you know what's wrong and how long it should take, they can soak you on the fees. And what are you going to do when they get 5-6 hours into a repair or project and then spring on you the news that it will take even longer than they anticipated to fix, costing you MORE money?

Always, always, always make sure you get a flat-rate, fixed fee quote (or "not to exceed" quote) in advance so you don't end up getting burned – and NEVER take a phone quote!

## **21 Questions You Should Ask Your IT Service Company Before Hiring Them to Support Your Network**

### **Customer Service:**

**Q1: Do they answer their phones live or do you always have to leave a voice mail and wait for someone to call you back?**

Any reputable IT service company will answer their phones live from at least 8:00 am to 5:00 pm and give their clients an emergency after-hours number they may call if a problem arises, including weekends. Why? Because many CEOs and executives work outside normal hours and find it to be the most productive time they have. If they cannot access their computer network AND can't get hold of anyone to help them, it's incredibly frustrating.

**Q2: Do they have a written, guaranteed response time to your calls?**

Your computer consultant must guarantee to have a technician working on your problem within a certain timeframe after you call. If they can't guarantee a certain response time, then be prepared to work on their timeframe and not yours when a problem does arise. A written guaranteed response time should be standard in every service agreement you sign.

**Q3: Do they take the time to explain what they are doing and answer your questions in terms that you can understand (not geek-speak), or do they come across arrogant and make you feel stupid for asking simple questions?**

Good technicians are trained to have the 'heart of a teacher' and will take time to answer your questions and explain everything in simple terms.

**Q4: Do they consistently (and proactively) offer new ways to improve your network's performance, or do they wait until you have a problem to make recommendations?**

Your service company should conduct quarterly or annual review meetings with you to look for new ways to help improve your operations, lower costs, increase efficiencies, and resolve any problems that may be arising. Their goal should be to help you be more profitable, efficient, and competitive with these meetings.

**Q5: Do they provide detailed invoices that clearly explain what you are paying for?**

Do you hate it when your IT service company sends you a bill and you have no idea what work was done? This is completely unacceptable behavior. You should demand that your service provider provide you with detailed invoices that show what work was done, why it was done, and when it was done so you never have to guess what you are paying for.

**Q6: Do they have adequate errors and omissions insurance as well as workers compensation insurance to protect YOU?**

Here's something to consider: if THEY cause a problem with your network that causes you to be down for hours or days or to lose data, who's responsible? Here's another question to consider: if one of their technicians gets hurt at your office, who's paying? In this litigious society we live in, you better make sure whomever you hire is adequately insured with both errors and omissions insurance AND workers compensation – and don't be shy about asking to see their latest insurance policies!

True Story: A few years ago, a "big box" store's IT Service Desk was slapped with a multi-million dollar lawsuits from customers for the bad behavior of their technicians. In some cases, their techs were accessing, copying, and distributing personal information they gained access to on customers' PCs and laptops brought in for repairs. In another case, they

lost a client's laptop (and subsequently all the data on it) and tried to cover it up. Bottom line, make sure the company you are hiring has proper insurance to protect YOU.

**Q7: Do they guarantee to complete projects on time and on budget?**

All projects should be a fixed priced and guaranteed to be completed on time and in writing. This is important because many unethical or incompetent computer guys will only quote "time and materials," which gives them free reign to nickel and dime you as well as take as much time as needed on completing a project.

### **Maintenance of Your Network:**

**Q8: Do they insist on remotely monitoring your network 24/7/365 to keep critical security settings, virus definitions, and security patches up-to-date and PREVENT problems from turning into downtime, viruses, lost data, and other issues?**

A remote network monitoring system watches over your network to constantly look for developing problems, security issues, and other problems so your computer consultant can address them BEFORE they turn into bigger problems and network downtime.

**Q9: Do they provide you with a monthly or quarterly report that shows all the updates, security patches, and status of the machines on your network so you know for SURE your systems have been secured and updated?**

Demand a detailed report that shows the overall health of your network and the updates to your antivirus, security settings, patches, and other important network checks (like hard drive space, backups, speed and performance, etc.). Even if you don't read through the report every time you receive it, it's important to know that this is happening.

**Q10: Is it standard procedure for them to provide you with written network documentation detailing what software licenses you own, critical passwords, user information, hardware inventory, etc., or are they the only person with the “keys to the kingdom?”**

Every business should have this in written and electronic form at no additional cost. Your IT service company should also perform regular updates on this material and make sure certain key people from your organization have this information and know how to use it, giving you complete control over your network.

Side Note: You should NEVER allow an IT person to have that much control over you and your company. If you get the sneaking suspicion that your current IT provider is keeping this under their control as a means of job security, get rid of them. This is downright unethical and dangerous to your organization, so don't tolerate it!

**Q11: Do they have other technicians on staff who are familiar with your network in case your regular technicians go on vacation or gets sick?**

Since they are keeping detailed network documentation and updates on your account, any of their technicians should be able to pick up where another one has left off.

**Q12: When they offer an “all-inclusive” support plan, is it TRULY all-inclusive, or are there “gotchas” hidden in the fine print?**

One of the more popular service plans offered by consulting firms today is an “all-inclusive” or “all-you-can-eat” managed services plan. These are actually a good thing because they'll save you a lot of money in the long run – HOWEVER, make sure you REALLY understand what is and isn't included. Some things to consider are:

- Is phone/e-mail help desk included, or extra?
- What about network upgrades, moves, or adding/removing users?

- Is hardware and/or software included?
- What about 3<sup>rd</sup> party software support? (We recommend that this IS included).
- What are the costs/consequences of early cancellation?
- What if you aren't happy with their services? Do they offer a money-back guarantee?
- If the hardware and software is included, what happens if you cancel the contract?
- Is offsite backup included? To what degree?
- If you have a major disaster, is restoring your network included or extra?
- What about onsite support calls? Or support to remote offices?

### **Backups and Disaster Recovery:**

**Q13: Do they INSIST on monitoring an offsite as well as an onsite backup, or are they letting you rely on outdated backup methods?**

I would never allow any business these days to use older backup methods because they are incredibly unreliable. Any backup software package more than three years old is lacking key features that could save a business from disaster.

**Q14: Do they INSIST on doing periodic test restores of your backups to make sure the data is not corrupt and could be restored in the event of a disaster?**

Your service company should perform a regular “fire drill” and perform a test restore from backup to make sure your data CAN be recovered in

the event of an emergency. After all, the WORST time to “test” a backup is when you desperately need it.

**Q15: Do they insist on backing up your network BEFORE performing any type of project or upgrade?**

While this may seem like common sense, you’d be surprised how many rookie technicians forget this important step. This is a simple precaution in case a hardware failure or software glitch causes a major problem.

**Q16: If you were to experience a major disaster, do they have a written plan for how your data could be restored FAST and/or enable you to work from a remote location?**

At minimum, you should have a simple disaster recovery plan for your data and network. I would also encourage you to do a full disaster recovery plan for your office, but at a minimum, your computer network will be covered should something happen.

### **Technical Expertise and Support:**

**Q17: Is their help-desk US based or outsourced to an overseas company or third party?**

An in-house help desk helps to ensure the folks helping you are friendly and helpful. We consider this one of the most important aspects of customer service, plus we feel it’s an important step in keeping your data secure.

**Q18: Do their technicians maintain current vendor certifications and participate in on-going training – or are they learning on your dime?**

Any technician working on your network should be up to date on the vendor certifications on your network (i.e. Microsoft, Cisco, etc.). Our

experience is that the vast majority of technicians out there these days are woefully undertrained.

**Q19: Do their technicians arrive on time and dress professionally?**

Any technician working on your network is a part of your staff while they are at your office. Are the technicians you're used to dealing with true professionals that you would be proud to have in your office? Do they dress professionally and show up on time?

**Q20: Are they familiar with (and can they support) your unique line of business applications?**

Any IT service company should "own" the problems with all of your line of business applications. That doesn't necessarily mean that they can fix faulty software – but they SHOULD be the liaison between you and your vendor to resolve problems you are having and make sure these applications work smoothly for you.

**Q21: When something goes wrong with your Internet service, phone systems, printers or other IT services, do they own the problem or do they say "that's not our problem to fix?"**

Your computer consultant should own the problem so that you don't have to try and resolve any of these issues on your own – that's just plain old good service and something many computer guys won't do.



**The SuperSTAR IT Service Company You Want  
vs A SuperSCREWup You Don't Want**

| <b>SuperSTAR</b>  | <b>SuperSCREWup</b>  |
|---|--|
| Has proven qualifications and experience, is vendor certified                         | Is just getting started, has no tangible qualifications                |
| Is fully insured (liability and worker's compensation)                                | Has no insurance   |
| Has several client references   | Has no references or testimonials                                      |
| Has multiple technicians  | Has no backup team, works alone  |
| Guarantees response times and has documented response systems in place                | Has no response system or guarantees, won't commit to anything         |
| Documents all discussions, deliverables, guarantees, and project timelines in writing | Prefers verbal communication, never follows up with written agreements |
| Uses detailed reporting   | Provides no reports or status updates                                  |

| SuperSTAR   | SuperSCREWup   |
|---|--|
| Has an established office   | Has no office, uses a PO box and a cell phone  |
| Provides all timelines, prices, and service level guarantees in writing                               | Provides vague project outlines, time and materials pricing, no timelines                    |
| Shows up on time  | Shows up late or not at all  |
| Sends correct, detailed invoices  | Invoices are incorrect, very difficult to read, never on time                                |
| Is easy to reach, returns calls promptly  | Is hard to reach   |
| Is always professionally dressed  | Is sloppy, has disheveled appearance   |
| Uses systematic follow-up to ensure your satisfaction   | Uses no follow-up, never hear from him unless you call with a problem                        |
| Solves problems quickly and professionally, stands behind all work for complete customer satisfaction | Is apathetic toward problem resolution, has no policies or procedures for resolving problems |

## **12 Warning Signs that You Hired the Wrong IT Service Company**

The service company:

1. Becomes defensive or argumentative when you ask about project costs or completion dates, or when you question their recommendations.
2. Won't guarantee their work or your satisfaction.
3. Talks down to you, uses "geek speak," and makes you feel stupid when you question their recommendations or work.
4. Is consistently late or rushed, and misses deadlines without an explanation or apology.
5. Leaves your office a mess (wires and cables exposed, furniture out of place).
6. Looks sloppy or disheveled.
7. Uses high-pressure or scare tactics to get you to buy.
8. Doesn't explain your options for resolving a problem or completing a project; it's basically their way or the highway.
9. Doesn't follow up after completing a project.
10. Conducts personal business or supports other clients from your office when they're supposed to be working on your project or network.
11. Never takes a proactive approach to supporting your network, and doesn't offer recommendations to help you secure your network, save money, or improve your company's productivity.
12. Doesn't offer a preventive-maintenance or monitoring program to ensure that your network is protected from viruses, hackers, data loss, downtime or other problems.

## 4 Mistakes to Avoid When Choosing an IT Service Company

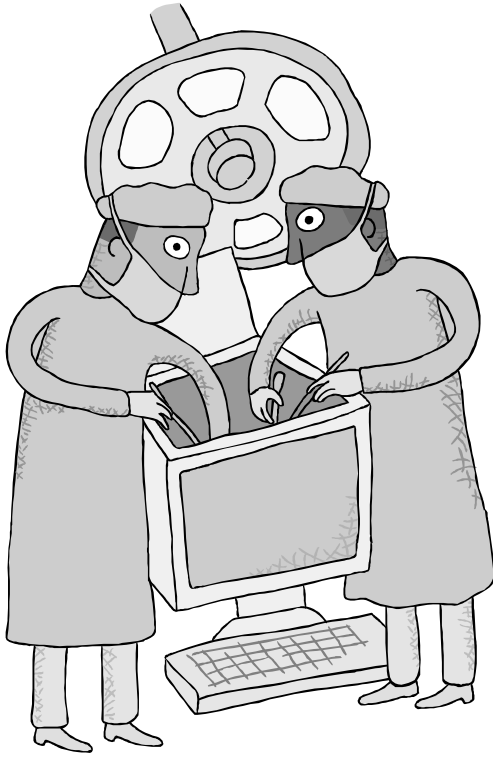
1. **Choosing an IT service company based on a single phone call.** We recommend you invite them into your office and ask them for a written proposal. Be clear on what your expectations are and what type of problems you want them to resolve. A competent professional should offer to do an audit of your network to diagnose your system BEFORE quoting you anything. After all, would you take a doctor's word that you need surgery if they hadn't done x-rays or other diagnostics? Of course not! Prescription without diagnosis is malpractice.
2. **Choosing an IT service company that doesn't have a written money-back guarantee.** In our view, a good consulting firm should be accountable for their services and fixing things RIGHT. If you aren't pleased with a job that was done, they should (at a minimum) make it right for no additional charge; and if they simply cannot resolve an issue to YOUR satisfaction, you shouldn't get stuck with the bill.

Plus, the fact that they stand behind their work with a money-back guarantee shows they have confidence in themselves to make you a happy client. And don't fall for the, "We don't offer one because people will take advantage of us" routine. In our experience, MOST people just want an honest service at a reasonable price. If you give them that, they are happy to pay. Are there a few unethical folks out there? Of course, but they are the minority, and we would rather bite the bullet on the very few dishonest folks so we can gain the trust and confidence of the majority of clients who just want their problems fixed fast and right.

3. **Choosing an IT service company without speaking to several of their current clients.** Check their references! Don't just take the sales guy's word that they are good – ask to speak to at least three clients that are similar in size and scope to you. If

they hesitate or cannot provide you with references, don't trust them! Another good sign is that they should have multiple client testimonials and success stories posted on their website and throughout their marketing collateral. A lack of this may be a sign that they don't have clients who are happy enough to provide a good reference – again, a warning sign.

4. **Choosing an IT service company that cannot remotely monitor, update, and support your network.** In this day and age, a computer consulting company who doesn't do this is living in the stone ages. You want someone to do this because it will dramatically increase your network's security and will enable them to do faster repairs. That's not to say they shouldn't come onsite; but remote monitoring and repairs make fixing problems **FASTER** for YOU and helps **AVOID** problems from cropping up in the first place.



# Chapter FOUR

## Avoiding Project Nightmares, Disasters, and Expensive Miscommunications

If you've ever been disappointed with a computer consultant's service, this chapter will be of great interest to you.

Small technical "glitches" or repairs can be incredibly frustrating because they seem so insignificant, yet they greatly interfere with your ability to get things done. In most cases, firm administrators may be under the assumption that these tiny problems can be solved quickly, which is not always the case.

If you've hired an incompetent IT service company before, you know that simple projects can turn into a full-day ordeal, and may even drag out for weeks or more. Unbelievably, your small repair can end up requiring multiple follow-up visits and calls because it occurs repeatedly, even after it has been "fixed." To make matters worse, the consultant will probably charge you for those extra visits, even if the issue should have been resolved the first time you paid him to fix it!

This doesn't even take into consideration the inconvenience and downright chaos this causes to your business. Unlike automobile and home repairs, computer network problems can completely disrupt your business, taking you offline for hours or even days.

Consider this scenario:

You hire a service company to upgrade your network, but their technicians are way over deadline, and you are still experiencing problems; only now, your phone calls aren't being returned promptly and the company is acting as if YOU are the problem. Then, to add insult to injury, they ask you for more money!

While you're sitting there waiting for your network to come back online or your project to be completed, your stress level is escalating through the roof because you know your deadlines and clients aren't going to wait, and it further irritates you that the company has not kept the promises they made so enthusiastically in the beginning.

Let's face it: You have a business to run, and you don't have the time to deal with technical issues or the incompetence of your consultants. Maybe you have a big proposal that needs to be submitted by the end of the day. Maybe you have sales leads or client orders that are getting colder by the minute and possibly even ruining client relationships. And, if you're like most firm administrators, you are already working behind schedule, so computer problems magnify the stress and delays to a whole new level.

If you've ever been through this type of nightmare, you know I'm not exaggerating. To prevent this from happening to you, or to avoid its happening again, you have to identify what causes these situations in the first place. That's what this chapter is all about.

## **Determine Your Priorities**

The first step to avoiding problems with an IT service company is to determine your "satisfaction priorities." Do you place a greater importance on response times or price? Is the quality of the work more important, or do you need it done fast? Is it critical that you have regular updates and status reports on your network, or is a quick e-mail now and again sufficient?

This is not to say that you can't have it all; but if fast response is a priority, you need to clearly communicate that to your consulting company *before* you hire them. You should also detail what you consider "fast" to mean.

Do you expect the company to return your call within 15 minutes or 4 hours? Do you expect them to be on-site the same day you call, or within the week? Make sure you are both clear before entering into an agreement. Some computer consulting firms may be more expensive, but may offer a higher quality of workmanship and customer service. Is that acceptable to you? Again, you need to determine this before entering into any project or agreement.

Once you've made a list of the qualities and characteristics that are most important to you, share this list with your prospective IT service company to help them customize their services to suit you.



## **A Quick Word on Price**

As with everything in life, you get what you pay for. The most expensive IT service company will not necessarily be the best, but you should be cautious if your #1 priority is price. As a consumer, you know firsthand that you are always being offered competitive pricing on services and products. Businesses compete hard for your dollars and it's only natural for you to think of price first when looking for computer repair and consulting services.

However, services can't usually be compared like tangible goods such as cars or office equipment. With products, you can equate features and benefits in an apples-to-apples comparison. With services, there are too many intangible aspects that can't be compared easily.

If what you really want is cheap computer support, you can practically guarantee that you're going to have problems. The price won't seem so attractive when you've lost every file on your computer, or if the work has to be redone when it's discovered that it wasn't completed right in the first place.

If you rely heavily on your computer network and the information it contains, it only makes sense to take time and choose the most *competent* service company possible, not the cheapest. Quality consultants can give you the expert advice and support you need. They can help lower your company's costs while increasing productivity, customer service, and sales. And they will be there when you need them.

## **Start Small**

Before you hire your IT service company to install a new network, hire them to do a small repair or network audit. This will give you the opportunity to see if they show up on time, follow through, and are enjoyable to work with. Never jump into a major project until you've been happy with the company's work on a smaller project.

## **Demand a Fixed Price**

Many IT service companies charge by the hour for projects instead of quoting a fixed rate. This works great for them, but is dangerous for you. Unless you have an established, high-trust relationship with your

service company (or a bottomless pit of money), don't agree to this type of contract. This gives your vendor a wide-open field to take as long as they want working on your project—and it actually benefits them if they do. Instead, ask them for a fixed fee that details exactly what results they will deliver for an agreed budget. Of course, you must allow your IT service company to perform a thorough review of any systems that will be affected by the scope of your proposed project. And don't be surprised if your IT vendor offers an estimate instead of a quote if the project relies on multiple vendors or your staff.

## **Get Everything in Writing**

Getting everything in writing is one of the most important things you can do to avoid getting taken advantage of by an incompetent or less-than-ethical consultant or service company. This includes:

- A project timeline and completion date
- A written service guarantee
- A budget and payment schedule
- Any and all expectations you have for deliverables
- When and how you will receive project updates
- Your responsibilities as the client
- What happens if you are not satisfied
- What happens if your project runs over the designated completion date

## **Do Your Research**

We've discussed what to look for—actually demand—from your IT service company. Some of those characteristics will need to be researched; don't skip those steps to save time. Ask your prospective vendor to provide the information you are looking for as part of their proposal. If they don't, or won't, cross them off your list of potential partners.

## **Communicate Your Concerns**

Some people are too shy to say what's really on their mind for fear of appearing rude or unreasonable. But if you have any concerns, questions, or reservations, you need to voice them to your prospective service company before signing the contract, and ask them to address *in the contract* how they will overcome those concerns if you hire them for the project.

If you are concerned that they won't return your calls fast enough, let them know. If you are afraid they might not be able to handle the job, be honest and tell them. You don't have to be harsh or disagreeable; simply let them know that you have a few concerns and ask what they can do to assure you that you won't be disappointed.

# Chapter FIVE

## How to Get the Most Out of Your IT Service Company

Now that we've defined what to look for in qualified, competent, honest consultants, it makes sense to tell you how to get the most out of your relationship with them.

A great service company will free you from worrying about data loss, downtime, or other problems, allowing you to focus on the more important, strategic aspects of running and growing your firm. It will also free your staff from trying to be jacks-of-all-trades and wasting time on activities they are not particularly good at, which also distracts them from doing their regular job. And ultimately, a good IT service company will recommend products and solutions to help your firm operate more competitively, increase sales, and lower your workload and stress levels.

But that is not to say you are completely off the hook.

There are a number of ways you can undo everything your consultants have done for you and severely jeopardize the security and reliability of your network. Plus, you are ultimately responsible for making sure your IT service company understands your firm priorities, goals, and operational systems so they can offer advice and solutions to support you.

Once you understand your role and responsibilities for maximizing your technology investments, and what your IT service company is and is not responsible for, you will have a much better working relationship with them and prevent most unpleasant surprises and expensive misunderstandings.

## Take Responsibility for Your Own Protection

Many firm administrators automatically blame their computer or their IT service company when they experience a problem, get infected with a virus, or realize their network has been taken over by spyware. And in some cases, these problems *are* due to negligence by your service company.

However, most spyware and virus attacks are the result of an end-user downloading a questionable file or program, disabling their antivirus software, or somehow circumventing security settings or acceptable-use policies set by your IT service company (such as visiting a peer-to-peer file-sharing network or installing games from social media websites).

Many other problems are due to hardware or software inadequacies that can't be controlled or prevented by your consultants. And finally, many firm administrators don't want to pay for their consultants to perform simple preventive maintenance, update security patches and virus definitions, or monitor their system's performance. This lack of maintenance is an invitation for problems that can't be blamed on your IT service company.

Unless your IT service company has *complete* control over your network and has been given the responsibility to monitor and maintain your network 24/7/365, chances are that your problems were not caused directly by some action they took (or didn't take). Again, that is not to say that you are completely at fault for all network problems, but you and your employees need to take an active role in keeping your network and data safe from harm.

We recently ran into an example of this with one of our oldest clients. This particular client has worked with our company for years, and has received a very good level of service from us. So, when we approached this client to discuss managed services and network monitoring, they declined. The client stated that they were happy with "break-fix" service and didn't see the need for regular maintenance and monitoring. For a while, their network appeared to be running well. However, they called one day in a panic. Their main server was down and no one could work. After dispatching a technician onsite, we found that the server was experiencing numerous problems. Among the database and backup problems, the server hadn't received the last 84 critical patches from Microsoft. This meant that their server was vulnerable to a number of security attacks and virus/spyware problems. The client was lucky that we were able to resolve the problems, but not before they were down for an extended period of time. The client was

also very fortunate that a backup wasn't needed or a virus wasn't introduced into their network.

## **Keep Spyware, Malware, and Viruses Off Your Network**

In almost every case, malware, spyware, and viruses (*see IT Dictionary at the end of this book for more info*) are able to invade a network because of some action taken by a user (or inaction). Cybercriminals are *incredibly clever* and have figured out ways to access your computer network through some of the most innocent and common activities you perform daily.

For example, many of the clients we see infected with spyware simply downloaded a screen saver, a coupon program, a web toolbar, an “enhanced” web browser, a music file, or some other “cute” program. In doing so, they also unknowingly downloaded a number of spyware and malware programs. Within a short time, they could no longer use their computer because of its slowness, instability, and pop-ups. Your IT service company can usually clean up the mess caused by these programs, but it is your responsibility to become educated about what you can and can't download. Below is a short list of programs and Websites you should never download or visit. Your consultants should be able to provide you with a more comprehensive, up-to-date list:

- Screen savers.
- “Enhanced” web browsers like Cool Search.
- Emoticons.
- Games.
- Peer-to-peer file-sharing software.
- Music files from non-trusted websites.
- “For fun” surveys (what type of person are you?).
- Banners that challenge you to “punch the monkey,” shoot something, or answer a trivia question to win a prize.
- Sweepstakes or drawings.
- Any software that requires you to accept certain conditions; by agreeing to their conditions, usually outlined in small print, you are agreeing to accept third-party software.

Unfortunately, installing the above programs is not the only way a hacker or malware program can access your computer network. If you don't have the most up-to-date security patches and virus definitions installed, wrongdoers can access your computer through a banner ad or even an e-mail attachment.

## **Be Aware of Sneaky Ways Hackers Invade Your Network**

Not too long ago, Microsoft released a security bulletin about three newly discovered vulnerabilities that could allow an attacker to gain control of your computer by tricking you into downloading and opening a maliciously crafted picture. At the same time, Microsoft released a Windows update to correct the vulnerabilities. But if you weren't testing and applying critical updates as soon as they became available, you were completely vulnerable to this attack.

Here's another compelling reason to ensure your network stays up-to-date on the latest security patches: Most hackers do not discover these security loopholes on their own. Instead, they learn about them when Microsoft, or any other software vendor for that matter, announces the vulnerability and issues an update. That is the hackers' cue to spring into action; they immediately analyze the update and craft an exploit (like a virus) that allows them access to any computer or network that has not yet installed the security patch. The time between the release of the update and the release of the exploit that targets the underlying vulnerability is getting shorter every day.

When the "nimda" worm was first discovered in the fall of 2001, Microsoft had released the patch that protected against that vulnerability *331 days before*. So network administrators had plenty of time to apply the update. Of course, many still hadn't done so, and the nimda worm caused lots of damage. Today, reports show that hackers can exploit vulnerabilities in less than a day, providing further proof that computer patches must be tested and installed much more regularly than ever before.

Clearly, *someone* needs to be paying close attention to your systems to ensure that critical updates are applied as soon as possible. That's why

we highly recommend that firm administrators allow their IT service company to monitor and maintain their network.

## **Create and Enforce an Acceptable-Use Policy (AUP)**

An Acceptable Use Policy (AUP) is a written document stating exactly what your employees can and can't do with company Internet access, computers, and e-mail. For example, employees should not be allowed to download or access screen savers, pictures, music files, or streaming music/video websites. This will save precious bandwidth and prevent downloading viruses and spyware. An AUP should also educate employees on the appropriate use of your company's resources.

If you don't want your staff to download pornographic material and send racist jokes through a company e-mail account, you have to communicate this information to them in an AUP and have them acknowledge *in writing* that they have read and understood it. Your IT service company can help you draft this document and enforce the policies outlined.

While recently working with a new client, the client mentioned slow internet speeds. Apparently, the solution from his previous IT service company had been to simply purchase more bandwidth from his internet service provider. After performing an audit on his network, we quickly found that many of the client's end-users were streaming music through the internet all day. In fact, one user was even streaming television shows because she liked the "white noise" in the background. Needless to say, a simple AUP quickly resolved the client's speed issues, and he was able to save money by lowering his data plan with his internet service provider.

## **Allow Your Consultant to Maintain Your Network**

As we mentioned previously, many firm administrators do NOT perform regular maintenance on their computer network; they basically use the network until it stops working, and then bring in their consultants.

While this arrangement may seem to work just fine in the short-term, it can dramatically increase problems and the costs of keeping



your network running. Then there is the threat of experiencing a major network disaster. Unfortunately, most businesses have to experience some type of catastrophe before they get serious about maintaining their network. Just ask any business owner about the importance of a solid backup or keeping their security up-to-date after they've gone through the devastation of losing a week's worth of work.

Look at these alarming statistics:

- Approximately **20%** of all small and medium-sized businesses endure a major network disaster **every five years**.
- The U.S. National Fire Protection Agency predicts that **43%** of companies that experience these disasters will never reopen, and another **29%** will close within three years.
- If the loss involves data, the diagnosis is even worse. According to the U.S. Bureau of Labor, **93%** of companies that suffer a significant data loss are out of business within five years.
- In April 2008, Symantec reported that there were over 1 million computer viruses in existence (and growing).
- The Internet Storm Center, which tracks security attacks, reports **7.6 million attacks** in the U.S. alone.

If you really want to protect yourself from data loss, viruses, spyware, hackers, downtime, and a host of other problems, the best thing you can do is find an IT service company that offers 24/7/365 monitoring and maintenance for your network, and then let them do it for you. By allowing your service company to control, manage, and maintain your network, the chances of experiencing significant problems is greatly reduced (more on this in the following chapter).

## **Be a Great Client**

There is a lot of truth in the cliché, “You’ll attract more bees with honey than vinegar.” This is especially true when working with professional consultants.

Quite often, firm administrators take an adversarial approach to working with their vendors. Since they are paying the bills, they believe that they have the right to be demanding, difficult, and even hostile. What they don’t realize is that vendor relationships can make or break a company, and maintaining a good working partnership with your IT service company is critical to your business success.

The more respect and appreciation you give your consultants, the more they will want to do a great job for you. Keep in mind that you might need them to do you a favor, or pull you out of a big mess, somewhere down the road. If you’ve developed a good working relationship based on mutual trust and appreciation, they will be far more willing to go the extra mile and help you out when you need it most.

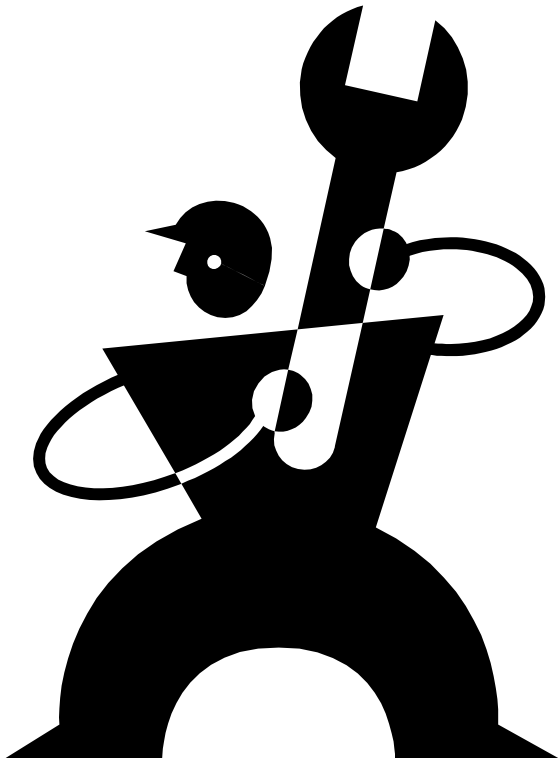
Here are three ways to make sure you become a “favorite” client who receives special favors and extra attention:

1. Pay bills on time or early.
2. Express your gratitude for the work they’ve done. Everyone likes to know that their efforts are appreciated.
3. If you have a complaint, don’t jump to the conclusion that your IT service company was trying to harm you on purpose. Let them know about your complaint and give them a chance to make it right before you get angry or take action. It may have been a simple mistake, or even an oversight, on your part.

Overall, clear communication is your best tool to ensure a great working relationship with your IT service company. You want to find a company you can partner with long-term who will take an active role in making your business profitable and successful. That requires mutual respect on both sides.

## **Six Ways a Good Relationship with a Competent IT Service Company Benefits Your Company**

1. The service company proactively monitors and maintains your network to prevent problems from happening, which gives you peace of mind by knowing that the “gremlins at the gate” are being watched and kept at bay.
2. The service company is familiar with your network and therefore can troubleshoot problems faster.
3. They understand your business and can recommend ways to save money, increase productivity, reduce mistakes, and service customers that you haven’t even considered.
4. They help lay a foundation for growing your business.
5. They know about any software or hardware that has been added to your network (which are frequently the source of problems).
6. They sort through all the new technological break-throughs, threats, and news, and only inform you of the things you need to know.



# **Chapter SIX**

## **Preventing Network Disasters with Proactive Maintenance**

The computers in your office and the network they reside on are, without a doubt, the single most important tools you use on a daily basis to run your business. Your computer network is at the core of your communications, operations, accounting, client care, and marketing. Just try to imagine one task or operation in your business that doesn't, directly or indirectly, depend on the security and availability of your computer network.

Yet, as important as your network is to your business, very few small-medium firm administrators take the necessary steps to ensure that it runs as smoothly and efficiently as possible. This is a huge, costly mistake.

With the constant changes to technology and daily development of new threats, even small peer-to-peer computer networks need ongoing maintenance and security updates from a highly trained IT service company.

Unfortunately, what we see most firm administrators doing is ignoring regular maintenance and only calling a service company when the network becomes inoperable. This reactive model of upkeep is a surefire path to extensive downtime, lost data, and spending more on IT support, not to mention major disruptions in worker productivity, sales, cash flow, production, and customer service that can never be recovered.

## **How Managed Services Can Prevent These Disasters from Happening to Your Business**

Thanks to advances in technology, your computer consultant can now provide ongoing remote maintenance and support to maximize the performance, reliability, and stability of your network. The industry term for this is “managed services,” although your IT service company might have a different name for it.

The basic premise is this: for a fixed monthly fee, your service company will take over the responsibility of performing regularly scheduled maintenance on your network to ensure that your virus protection and security patches are up-to-date, your backups are working properly, your firewall and other security settings are actively protecting you, the speed and performance of your network are maximized, and all the components of your network are functioning properly.

In essence, they are taking over the tactical, day-to-day maintenance and support of your network for a fraction of the cost of hiring a full-time consultant. While this is obviously the case for small businesses, we've found that many larger businesses with 100, 200, or even more employees can save money with outsourced IT service companies.

## **What Are The Benefits Of Managed Services?**

Service calls to computer networks not under a managed-service plan (MSP) require two to three times as long to diagnose and repair as systems that are under a MSP due to the time required for diagnostics and testing. This naturally leads to higher repair bills and more downtime.

In addition to the added expense and hours required for these repairs, some of the damage to your network can be irreversible, and could have been easily prevented with a solid MSP.

If the data and operation of your network are important to your business, you need to make sure you are taking the necessary steps to ensure its safety and security. A good managed-service plan will provide the following benefits:

- **You'll practically eliminate expensive repairs and data recovery costs.** By detecting and preventing network disasters before they happen, a good MSP will save you thousands of dollars in repairs and downtime.
- **You'll receive faster support.** Thanks to remote-monitoring software, your service company will be able to securely access and repair most network problems right over the Internet. No

more waiting around for a consultant to show up or paying for travel fees.

- **You'll experience faster performance, fewer problems, and practically zero downtime.** Some components of your network will degrade in performance over time, causing it to slow down, hang up, and crash. The regular preventive maintenance offered through an MSP will make sure your computers stay in tip-top shape for maximum speed, performance, and reliability.
- **You'll get top-level IT support without the costs and overhead of hiring a full-time IT manager.** A junior technician can easily cost your company \$45,000-50,000 a year in salary, taxes, and insurance, and a senior consultant could cost two to three times that amount. Under an MSP, you get to share senior consultants with other businesses, which greatly reduces your costs without sacrificing experience or quality of work.
- **You'll receive discounts on new projects and better service.** Most IT service companies will offer priority service and a discount to clients on their managed-service plan. Plus, your consultants will become more familiar with your hardware, software, settings, and history, and therefore provide faster service than the consultants who have to spend time “feeling around” your network.
- **You can budget for IT support just like rent or insurance.** If your IT support bill varies from month to month, a managed-service plan will help even it out and make budgeting easier. Just make sure the plan you sign up for is all-inclusive, with no hidden charges, caveats, or fees.
- **You will safeguard your data.** The data on the hard disk is always more important than the hardware that houses it. If you rely on your computer system for daily operations, it's time to get serious about protecting your critical, irreplaceable

electronic information. A good MSP will greatly reduce your chances of losing critical company data, files, and information.

- **You'll gain peace of mind.** As a business owner, you already have enough to worry about; the last thing you need is a computer crisis. Having a managed-service plan in place takes that worry off your plate.

## **What to Look For In a Managed-Service Plan**

There are a number of factors to look for in a MSP. A good IT service company will take time to sit down with you and explain the options, based on your priorities, budget, network complexity, support needed, and conditions of satisfaction. However, here are a few things to make sure your service company includes in your agreement:

- **Security Patches and Updates.** Software vendors frequently issue critical patches to cover known security loopholes in their software. However, not all patches are trouble-free, and some will require specialized knowledge to install. On many occasions, Microsoft has distributed patches that come with fine-print instructions warning the user to install and test the patch on one machine before rolling it out to all the computers on the network. Since most people don't read the fine print on a software download, or are simply not aware of the problems that can arise from installing an untested patch, they blindly install it on their entire network only to discover that it caused a number of software conflicts and system failures. That's why it makes sense to allow a trained professional to manage and install patches on a regular basis. Trying to do this on your own is similar to playing Russian roulette with your network.
- **24/7/365 Monitoring and Alerts.** Your service company should be able to provide around-the-clock monitoring for your network to look for problems developing under the radar. They should also notify you of problems in advance so that preventive action can be taken.



- **Spam Filtering.** Not only is spam annoying, it is the number-one way viruses enter a computer network.
- **Virus Updates.** Unless you've been living under a rock, you know that viruses are a real, and very dangerous, threat to your computer network. Since new viruses launch daily, you need to make sure your service company is also monitoring your virus protection, and automatically updating your network with new virus definitions as soon as they become available. **Note:** Many IT service companies include antivirus software in their MSPs.
- **Spyware Scanning and Removal.** Like viruses, spyware can cause a number of problems for your network and may even result in identity theft. Symptoms of spyware include excessive pop-up ads, sluggish performance, and strange web browsers opening on your computer that you did not request.
- **System Backup Monitoring.** Your service company should monitor your daily system backups to make sure they are working properly and perform a regular test restore to make sure your data is available in a usable format. Tape backups are notorious for failing. Even if they appear to be working, the data could be corrupt and useless. We have seen several situations where a company thought their data was secure only to find out that it wasn't when they desperately needed it. **Note:** Most consultants will offer an off-site data backup solution for maximum "peace of mind."
- **Vendor Liaison.** Quite often, software or hardware will just fail. It's far more convenient to have a service company who is familiar with your network to deal with the warranty returns and replacements of those parts with the manufacturer, rather than deal with it yourself. If you've ever had to call the "customer service" hotline of a technology vendor, you know what a headache it can be. Other vendors include practice-management software, Internet Service Providers, Web-hosting companies, and so on. For

convenience, have your IT service company agree to be your vendor liaison with these companies so you don't have the hassle.

- **Creation of Acceptable-Use Policies and Training.** An acceptable-use policy is simply the rulebook for what your employees can and can't do with their computers. Uneducated employees can accidentally introduce spyware, viruses, hackers, and other major problems into your network. They can also use their work computer and e-mail to access and share unacceptable material. All it takes is one employee to send an off-color joke to a list of friends from your company's e-mail to start problems for you. In some cases, employees' actions can bring expensive and embarrassing lawsuits against your company. Talk to your IT service company about ways to educate and enforce an acceptable-use policy.
- **Adding and Removing Hardware and Software.** You just purchased a new printer and you're eager to start using it. However, you can't figure out why you keep getting error messages and why you can't print from Excel. If you had a managed-service contract that covered hardware and software installation, your consultant would be responsible for making sure it was installed and configured properly, and you wouldn't have to waste one minute dealing with these problems.
- **Adding and Removing Users.** Although this seems like a simple thing, user access to your network is a critical security risk that needs to be managed properly to avoid disgruntled employees or unauthorized persons accessing it. This is especially true if you have remote workers. **Note:** We recommend an "employee termination checklist" that outlines the steps to take when an employee leaves your organization.
- **Help Desk Support.** This would include a mix of phone, remote, and on-site support for you and your employees to

answer any number of technical questions and problems. Remember, unless specifically stated, phone support may not be free; calling your consultant for a “quick” question is a billable event and can cost you \$25-100. Therefore, you want to have some level of remote and on-site support included in your managed-service contract.

Keep in mind that this is just a starter list of services to look for. The size and complexity of your network, the security required, and the software and systems you use will largely determine the type of ongoing support you need. A good computer consultant will take time to understand your needs and offer a plan to meet your business’s requirements.

# Chapter SEVEN

## Moving to the Cloud

Undoubtedly you've heard all the commotion around cloud computing and how it's the "next big thing." Yet, despite all the hype, few people really seem to understand what cloud computing is or how it can help your business.

That's why I wanted to set the record straight and explain what cloud computing is, how it can (possibly) help your business, and if so, what you need to know in order to make good decisions about choosing a vendor.

Why "possibly?" Because cloud computing is NOT a good fit for every company; and if you don't get all the facts or fully understand the pros and cons, you can end up making some VERY poor and expensive mistakes that you'll deeply regret later.

That said, for some clients, cloud can actually lower IT costs by 15-25%, greatly improve the ability for remote workers to connect and work, simplify your entire IT infrastructure, and genuinely solve a number of technology problems that you've been trying to work around for years.

So which are YOU? By the end of this chapter you'll know, or at least have a much better understanding.

## 5 Critical Facts You Must Know Before Moving to the Cloud

In this chapter I'm going to talk about **5 very important facts you need to know before you consider cloud computing for your company.** This includes:

1. What is cloud computing?
2. The pros AND cons of this technology.
3. The various types of cloud computing options available (there is more than just one).
4. Answers to important, frequently asked questions.

5. What questions you need to ask your IT pro before letting them “sell” you on moving all or part of your network and applications to the cloud.

## What is Cloud Computing?

Wikipedia defined cloud computing as “The use and access of multiple server-based computational resources via a digital network (WAN, Internet connection using the World Wide Web, etc.).”

### But what the heck does that mean?

The easiest way to not only understand what cloud computing is but also gain insight into why it’s gaining in popularity, is to compare it to the evolution of public utilities. For example, let’s look at the evolution of electricity.

Back in the industrial age, factories had to produce their own power in order to run machines that produced the hard goods they manufactured. Be it textiles or railroad spikes, using machines gave these companies enormous competitive advantages by producing more goods with fewer workers and in less time. For many years, the production of power was every bit as important to their company’s success as the skill of their workers and quality of their products.

**Unfortunately, this put factories into TWO businesses:** the business of producing their goods and the business of producing power. Then the concept of delivering power (electricity) as a utility was introduced by Thomas Edison when he developed a commercial-grade replacement for gas lighting and heating using centrally generated and distributed electricity. From there, as they say, the rest was history.

The concept of electric current being generated in central power plants and delivered to factories as a utility caught on fast. This meant manufacturers no longer had to be in the business of producing their own power. **In fact, in a very short period of time, it became a competitive necessity for factories to take advantage of the lower cost option being offered by public utilities.** Almost overnight, thousands of steam engines and electric generators were rendered obsolete and left to rust next to the factories they once powered.

What made this possible was a series of inventions and scientific breakthroughs – but what drove the demand was pure economics. Utility companies were able to leverage economies of scale that single manufacturing plants simply couldn't match in output or in price. In fact, the price of power dropped so significantly that it quickly became affordable for not only factories but every single household in the country.

Today, we are in a similar transformation following a similar course. The only difference is that instead of cheap and plentiful electricity, advancements in technology and Internet connectivity are driving down the costs of computing power. With cloud computing, businesses can pay for “computing power” like a utility without having the exorbitant costs of installing, hosting, and supporting it.

In fact, you are probably already experiencing the benefits of cloud computing in some way but haven't realized it. Below are a number of cloud computing applications, also called SaaS or “software as a service,” you might be using:

- Gmail, Hotmail, Yahoo, or other free e-mail accounts
- Facebook
- NetSuite, Salesforce
- Constant Contact, Exact Target, Aweber, or other e-mail broadcasting services
- Zoomerang, SurveyMonkey, and other survey tools
- LinkedIn
- Twitter
- All things Google (search, AdWords, maps, etc.)

If you think about it, almost every single application you use today can be (or already is being) put “in the cloud” where you can access it and pay for it via your browser for a monthly fee or utility pricing (or sometimes even free). You don't purchase and install software but instead access it via an Internet browser.

## What about Office 365 and Google Apps?

Microsoft's Office 365 and Google Apps are perfect examples of the cloud computing trend; for an inexpensive monthly fee, you can get full access and use of Office applications. And, since these apps are being powered by the cloud provider, you don't need an expensive desktop with lots of power to use them – just a simple Internet connection will do on a laptop, desktop, or tablet.

Of course, these aren't great options for all businesses. Google Apps doesn't (currently) integrate with many line-of-business applications, which presents a deal breaker for using this service. For example, if you like using Microsoft's Excel or Word to pull reports or create documents from your line of business application, you might not be able to do that with Google Apps.

Microsoft's Office 365 is Microsoft's most popular cloud offering. It includes access to hosted email (Exchange), online file sharing, and even secure instant messaging. And while Microsoft doesn't offer much in the way of support, your IT service company should be well versed in this new technology.

## Pros and Cons of Moving to the Cloud

As you read this section, keep in mind there is no “perfect” solution. All options – be it an in-house network or a cloud solution – has both upsides and downsides. And which option works best for you has to be determined on a case-by-case scenario. (**Warning:** Do not let a cloud expert tell you there is only “one way” of doing something.) Most companies end up with a hybrid solution where some of their applications are in the cloud and some are still hosted and maintained from an in-house server. We'll discuss more of this in a later section; however, here are the general pros and cons of cloud computing:

## Pros of Cloud Computing:

- **Lowered IT costs.** This is probably the single most compelling reason companies choose to move their network (all or in part) to the cloud. You can save money on software licenses, hardware (servers and workstations), and in IT support and upgrades. In fact, we save our clients an average of 15% when we move some or part of their network functionality to the cloud. So if you hate constantly writing big checks for IT upgrades, cloud computing may be right for you.
- **Ability to access your desktop and/or applications from anywhere and any device.** If you travel a lot, have remote workers, or prefer to use a tablet while traveling and a laptop at your house, cloud computing will give you the ability to work from any of these devices.
- **Disaster recovery and backup are automated.** The server in your office is extremely vulnerable to a number of threats including viruses, human error, hardware failure, software corruption, and, of course, physical damage due to a fire, flood, or other natural disaster. If your server was in the cloud and (God forbid) your office was reduced to a pile of rubble, you could purchase a new laptop and be back up and running within the same day. This would NOT be the case if you had a traditional network and were using tape drives, CDs, USB drives or other physical storage devices to back up your system.

Plus, like a public utility, cloud platforms are far more robust and secure than your average business network because they can utilize economies of scale to invest heavily into security, redundancy, and failover systems making them far less likely to go down.

- **It's faster, cheaper, and easier to set up new employees.** If you have a seasonal workforce or a lot of turnover, cloud



computing will not only lower your costs of setting up new accounts, but it will make it much faster.

- **It's a "greener" technology that will save on power and your electric bill.** For some smaller companies, the power savings will be too small to measure. However, for larger companies with multiple servers who are cooling a hot server room and keep their servers running 24/7/365, the savings could be considerable.

## **Cons of Cloud Computing:**

- **The Internet going down.** While you can mitigate this risk by using a commercial grade Internet connection and maintaining a second backup internet connection, there is a chance that you'll lose Internet connectivity, making it impossible to work.
- **Data security.** Many people don't feel comfortable having their data in some offsite location. This is a valid concern, and before you choose any cloud provider, you need to find out more information about where they are storing your data, how it's encrypted, who has access to your data, and how you can get it back. You'll find more information on this subject under the "What To Look For When Hiring a Cloud Integrator" section later on in this book.
- **Certain line-of-business applications won't work in the cloud.** We've found that some graphics intensive applications or large database applications don't always work well in a cloud environment. Make sure you specifically ask about your line of business applications if you're thinking of moving to the cloud.
- **Compliance Issues.** There are a number of laws and regulations such as Gramm-Leach-Bliley, Sarbanes-Oxley, and HIPAA that require companies to control and protect their data and certify that they have knowledge and control over who can access the data, who sees it, and how and where it is stored. In a public cloud environment, this can be a problem. Many cloud providers won't tell you specifically where your data is stored

(geographically).

Most cloud providers have SAS 70 certifications which require them to be able to describe exactly what is happening in their environment, how and where the data comes in, what the provider does with it, and what controls are in place over the access to and processing of the data; but as the business owner, it's YOUR neck on the line if the data is compromised so it's important that you ask for some type of validation that they are meeting the various compliance regulations on an ongoing basis.

## **Different Types Of Cloud Solutions Explained:**

**Pure Cloud:** This is where all your applications and data are put on the other side of the firewall (in the cloud) and accessed through various devices (laptops, desktops, iPads, phones) via the Internet.

**Hybrid Cloud:** Although “pure” cloud computing has valid applications, for many, it's downright scary. And in some cases is NOT the smartest move due to compliance issues, security restrictions, or performance issues. A hybrid cloud enables you to put certain pieces of your existing IT infrastructure (e.g. storage and e-mail) in the cloud, and the remainder of the IT infrastructure stays on premise. This gives you the ability to enjoy the costs savings and benefits of cloud computing where it makes the most sense without risking your entire environment.

**Point Solutions:** Another option would be simply to put certain applications, like SharePoint or Microsoft Exchange, in the cloud while keeping everything else onsite. Since e-mail is usually a critical application that everyone needs and wants access to on the road and on various devices (tablet, smart phone, etc.) then often this is a great way to get advanced features of Microsoft Exchange without the cost of installing your own in-house Exchange server.

**Public Cloud Vs. Private Cloud:** A public cloud is a service that anyone can tap into with a network connection and a credit card. They are shared infrastructures that allow you to pay-as-you-go and are

managed through a self-service web portal. With a Public Cloud, your data is often stored on the same hardware as other businesses' data (e.g. Dropbox). Private clouds are essentially self-built infrastructures that mimic public cloud services, but are usually limited to a single client. Private clouds are often the choice of companies who want the benefits of cloud computing, but don't want their data held in a public environment.

## **FAQs about Security, Where You Data Is Held, and Internet Connectivity**

**Question:** What if my Internet connection goes down for an extended period of time?

**Our Answer:** This is a valid concern. We always recommend a redundant internet connection if your business relies on the cloud. In fact, many new routers can automatically switch to your backup internet provider in the event that your main internet connection goes down. Of course, you must factor in the cost of a second internet connection when determining if the Cloud will truly be a cost savings.

**Question:** What about security? Isn't there a big risk of someone accessing my data if it's in the cloud?

**Our Answer:** In many cases, cloud computing is a MORE secure way of accessing and storing data. Just because your server is onsite doesn't make it more secure; in fact, most small to medium businesses can't justify the cost of securing their network the way a cloud provider can. And most security breaches occur due to human error; one of your employees downloads a file that contains a virus, they don't use secure passwords, or they simply e-mail confidential information out to people who shouldn't see it. Other security breaches occur in on-site networks because the company didn't properly maintain their own in-house network with security updates, software patches, and up-to-date anti-virus software. That's a FAR more common way networks get compromised versus a cloud provider getting hacked. As an added precaution, we recommend private cloud options to further insulate our clients from security breaches.

**Question:** What if YOU go out of business? How do I get my data back?

**Our Answer:** We give every client access to their network documentation that clearly outlines where their data is and how they could get it back in the event of an emergency. This includes detailed information of emergency contact numbers, information on how to access your data and infrastructure (although our plan is always to be there to support you), a copy of our insurance policy, and information regarding your backups and licensing.

We also give you a copy of OUR disaster recovery plan that shows what we've put in place to make sure we stay up and running.

In fact, you should never hire ANY IT professional that won't give you that information.

**Question:** Do I have to purchase new hardware (servers, workstations) to move to the cloud?

**Our Answer:** No! That's one of the selling points of cloud computing. It allows you to use older workstations, laptops, and servers because the computing power is in the cloud. Not only does that allow you to keep and use hardware longer, but it allows you to buy cheaper workstations and laptops because you don't need the expensive computing power required in the past.

**Question:** Is the cloud right for me?

**Our Answer:** It depends. We've found that moving applications to the cloud can make sense for almost every small-medium business. Services such as company email and document sharing are logical places to start. However, to move a business to a "Pure Cloud" environment which "fork-lifts" their entire network and moves it to the cloud is still relatively expensive. However, as pricing for shared computing continues to decrease, you'll see more and more businesses moving to the cloud.

## What to Look For When Hiring a Cloud Integrator

A “cloud integrator” is a fancy name for an IT service company who sets up and integrates the various software and solutions into a cloud service specific for your business. But buyer beware! The cloud is relatively new technology, and you don’t want just anyone setting you up on this.

Unfortunately, as I’ve mentioned before, the computer repair and consulting industry (along with many others) has its own share of incompetent or unethical people who will try to take advantage of trusting firm administrators who simply do not have the ability to determine whether or not they know what they are doing. Sometimes this is out of greed for your money; more often it’s simply because they don’t have the skills and competency to do the job right but won’t tell you that up front because they want to make the sale.

From misleading information, unqualified technicians, and poor management, to terrible customer service, we’ve seen it all...and we know they exist in abundance because we have had a number of customers come to us to clean up the disasters they have caused.

Automotive repair shops, electricians, plumbers, lawyers, realtors, dentists, doctors, accountants, etc. are heavily regulated to protect the consumer from receiving substandard work or getting ripped off. However, the computer industry is still highly unregulated and there are few laws in existence to protect the consumer – **which is why it’s so important for you to really research the company or person you are considering to make sure they have the experience to set up, migrate, and support your network in the cloud.**

Anyone who can hang out a shingle can promote themselves as a cloud expert. Even if they are honestly *trying* to do a good job for you, their inexperience can cost you dearly in your network’s speed and performance or in lost or corrupt data files. To that end, here are five questions you should ask your IT person before letting them migrate your network to the cloud:

## **5 Critical Questions to Ask Your IT Service Company BEFORE Letting Them Move Your Network to the Cloud**

**Q1: How many clients have you provided Cloud services for to date?**

**Why you should ask:** You don't want someone practicing on your network.

**Q2: How quickly do they guarantee to have a technician working on an outage or other problem?**

**Why you should ask:** Anyone you pay to support your network should give you a written SLA (service level agreement) that outlines exactly how IT issues get resolved and in what time frame. I would also request that they reveal what their average resolution time has been with current clients over the last 3-6 months.

They should also answer their phones live from 8:00 a.m. to 5:00 p.m. and provide you with an emergency after-hours number that you may call if a problem arises, including weekends.

If you cannot access your network because the Internet is down or due to some other problem, you can't be waiting around for hours for someone to call you back OR (more importantly) start working on resolving the issue. Make sure you get this in writing; often cheaper or less experienced IT service companies won't have this or will try and convince you it's not important or that they can't do this. Don't buy that excuse! They are in the business of providing IT support so they should have some guarantees or standards around this that they can share with you.

**Q3: What's your plan for transitioning our network to the cloud to minimize problems and downtime?**

**Why you should ask:** Make sure that they run a simultaneous cloud environment during the transition and don't "turn off" the old network until everyone is 100% confident that everything has been transitioned and is working effortlessly. You don't want someone to switch overnight without setting up a test environment first.

**Q4: Where will your data be stored?**

**Why you should ask:** You should receive full documentation about where your data is, how it's being secured and backed up, and how you could get access to it. Essentially, you don't want your cloud provider to be able to hold your data (and your company) hostage.

**Q5: How will your data be secured and backed up?**

**Why you should ask:** If they tell you that your data will be stored in their own co-lo in the back of their office, what happens if THEY get destroyed by a fire, flood, or other disaster? What are they doing to secure their office? Are they backing it up somewhere else? Make sure they are SAS 70 certified and have a failover plan in place to ensure continuous service in the event that their location goes down.

# **Chapter EIGHT**

## **Contracts, Payment, Schedules, and Rate Negotiations**

Now that you've gone through the work of finding the perfect IT service company, make sure you don't throw all your hard work down the drain by not securing a clear, concise, win-win contract. It's your best defense against being ripped off and disappointed. It also helps both sides completely understand what is expected, how the work will be done, and your acceptable standards. In some instances, it makes sense to have a qualified attorney review your contracts; however, this chapter will outline some of the basics to include in your contract to make sure you get what you want.

In general, the more detailed the contract is, the better it is for both sides. Don't be afraid of lengthy contracts that spell everything out in specific detail, but DO be cautious of contracts you don't understand.

Once you've decided on a service company, ask to meet with them to go over every detail verbally. It's a good idea to prepare for this meeting by outlining your expectations and conditions of satisfaction for the work to be done. The clearer you are on what you want and how you want the work performed, the better your chances are of getting it done right. You should also ask your service company to bring a copy of the original proposal or quote, as well as a list of deliverables, deadlines, guarantees, and other policies and procedures.

This meeting is best done in a face-to-face setting. You can discuss your contract over the phone, but our experience shows that greater clarification and detail comes when we meet with our clients.

## **Warranties, Guarantees, and Making Things Right**

One of the main things you want to clarify in your contract is exactly what your IT service company does and does not guarantee. Make sure you are as specific as possible. For example, if a computer you purchase through your service company has a hard-drive failure, will they be responsible for getting it replaced with the manufacturer, or will you be?



If you experience a problem with the network your service company recently upgraded or installed, is support included, or charged at an extra rate? Also, if you are unhappy with the work, what happens? Will they redo the job at no extra charge?

## **Payment Terms**

As we mentioned in Chapter 3, an IT service company will usually require some type of down payment on a project before they get started, and payment for any hardware or software purchases up front. However, you should never pay in full before a project is started, and you should not be asked to pay the balance of a project until it is completed to your satisfaction. As a rule of thumb, try to reserve 50% of the payment until full completion of the project. Basically, you want to keep the final payment to make sure your consultant stays “on the ball” and eager to complete your project.

Regardless of what you agree on, your payment schedule should be detailed in a written contract. This includes exact payment milestones, amounts, and specifically what work and conditions of satisfaction have to be met before payment is made. Don’t be alarmed if your IT service company includes a condition that all work will cease for nonpayment. This is standard and not unreasonable.

## **Project Timeline and Completion Date**

If your project is time-sensitive, you’ll want to include a definite completion date. Include the phrase that your project is “extremely time-sensitive” and stress the importance of the completion date in writing.

If your project is lengthy, it makes sense to have a project timeline that includes benchmarks, or the phases that your project will be completed in, and payments tied to the completion of these. This will keep your consultant on track and prevent you from realizing in the 11<sup>th</sup> hour that your project is way overdue.

**Important:** Some projects will require your involvement in testing and approving applications and processes designed by your service

company. Make sure you allot time in your busy schedule for testing so you don't delay the project.

## **Changes, Modifications, and “Scope Creep”**

Scope creep is a term used by consultants to describe the changes and modifications clients request to a project after the contract has been signed. In some cases, these “tiny” changes result in more work for the IT service company and delays in the project's timeline.

For example, let's suppose you decide it's time to upgrade your network. Your IT service company provides you with a game plan and a quote for what it will take to upgrade your entire system. However, halfway through the project, you decide that you want to give your traveling sales team secure remote access to the network—something that was not discussed in the original project and proposal. Although it seems to be a simple request, it may take additional hardware, software, and hours of work to set up.

Therefore, it's normal and customary for a consultant to outline an hourly rate for all projects, changes, and tasks requested by the client *after* the contract has been signed. Just make sure that the hourly rate or amount for any changes is not unreasonable, *and* that it is clearly defined in the contract you sign. In most cases, the IT service company will agree to a discounted rate for additional work resulting from changes you make to the original agreement. Again, be sure you have that rate in writing so they don't double the rate halfway into your project.

**Word of caution:** Whenever you request a change to your existing contract or scope of work, make sure you get the change order in writing. If your IT service company is professional, they will ask you to sign a written contract addendum; but if they don't, make sure you press for one. Don't fall into the trap of verbal “he said, she said” agreements; they will only come back to haunt you. All change orders should include:

- The specific changes to be made
- The date of the request
- A detailed description of the work to be done

- Your conditions of satisfaction
- The additional charges
- Guarantees or warranties
- A new completion date for your project (if necessary)

This document should be signed by both you and your IT service company.

## **Hardware, Software, and Materials**

Many IT service companies will gladly research and quote the cost of various hardware and software for the completion of a project. In most cases, we always recommend “Tier 1” equipment (e.g. Dell, HP, IBM, etc.).

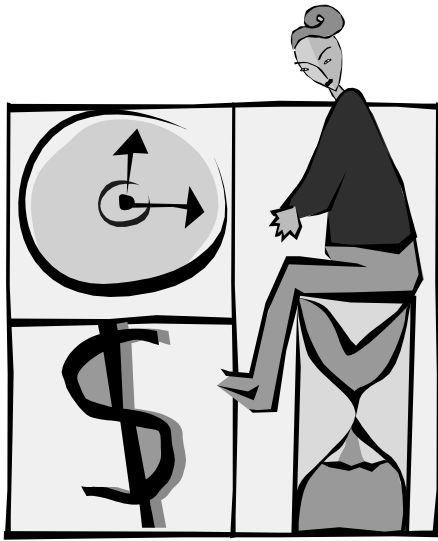
If your consulting company “custom builds” equipment for you, make sure you get details in your contract regarding who is responsible for the warranty on the equipment. If something goes wrong, do you want your IT service company to handle it, or will you? Most service companies will charge for handling the warranty repairs on your equipment; don’t make the mistake of assuming that, because they sold it to you, they are responsible for manufacturer defects, or that they will do the repairs for free. If you expect them to handle this, you must detail that in your contract.

## **Hours and Conditions of Work**

Another point you want to consider before signing on the dotted line is how and when the work will be completed. One of the biggest inconveniences of having an IT service company work on your network is the downtime it costs you.

In some situations, it may be necessary for you and all of your employees to log off the network so your provider may complete certain tasks. If you only need to log off for a short time, it’s probably a minor inconvenience; however, if you are upgrading your entire network, or installing a new system, you could be down for several hours.

To prevent your business from being disrupted for long periods, ask your IT service company how much downtime the repair or project will require. If you can't afford to be offline for that long, ask that any major upgrades, installations, or repairs be done after hours or on weekends. It may cost a bit more, but most IT service companies will gladly accommodate you if you ask in advance.



# STAY SECURE

## Computer Security

1. Always use an antivirus program. A properly installed antivirus program that is getting daily updates will stop the majority of malicious software from infecting your computer.
2. Make sure you're downloading the latest software security patches from Microsoft, Adobe, Java, and other vendors. If you're concerned about installing a patch that hasn't been thoroughly tested, consider using a third-party patch lab (we do).
3. Backup your data. Even if you're backing up your company's server every night, your desktop computer may have company information that isn't being backed up regularly.
4. In addition to a daily local backup, backup your data offsite EVERY day. With the price of cloud backups and BDRs (see I.T. Dictionary in the next section), there's no reason not to have a local copy and an offsite copy of your company's data.
5. Encrypt your computers' hard drives. This will insure that only authorized users will be able to access your data.
6. Use strong passwords!
  - a. Make your passwords as long as possible. Today, eight character passwords are considered the minimum. Many security experts recommend at least 15 characters.
  - b. Use different types of characters (e.g. numerals, lowercase letters, uppercase letters, symbols).
  - c. Don't use words that appear in a dictionary.
  - d. Don't use your username.
  - e. Don't write your password down. You'd be surprised by how often I've seen a user's password taped to their computer monitor.
  - f. Change your passwords often.
  - g. Don't tell anyone your password.
  - h. If possible, don't use your password on a public computer.

## **Network Security**

1. Always use a firewall. Besides blocking unwanted traffic from outside of your network (i.e. hackers), many firewalls include VPN connection capabilities.
2. If using a wireless network, make sure it is password protected. In fact, if the wireless network is in high-traffic areas, consider changing the password on a regular basis.

## **Email Security**

1. Setup a company policy on email forwarding. Never forward a chain letter email or a virus warning of any kind to any user (other than your IT service provider).
2. Use email filtering software to stop spam and email that may contain malicious software.
3. Never make a purchase through an unsolicited email. You never know who you're giving your credit card information to!
4. Don't share your email address on your website. This is an invitation to spammers.
5. Don't use the "preview" pane in Outlook.
6. If you email a group, consider using the BCC field when appropriate. By using "blind carbon copy," you'll prevent your recipients from seeing (and saving) the email addresses of other recipients on your email message.
7. Never respond to email messages that request your personal financial information. If a message asks for your bank account number or PIN number, don't give it to them.

## **Internet Security**

1. Use different passwords for every site. If this presents too great a challenge, consider using a secure password storage site.
2. Use content filtering software/hardware for your office network. A content filtering mechanism can stop users from surfing to

inappropriate websites or websites that could be known for containing malicious software.

3. Don't click on pop-ups!

## **Mobile Security**

1. Stop whatever you're doing and put a password (lock) on your phone, tablet, and laptop NOW.
2. If you're a business owner, use Mobile Device Management software to keep track of your employees' portable devices and erase them if they're lost.



# ***I.T. Dictionary***

## **Technical Terms Explained in Plain English**

**AdWare:** software that displays advertising and/or pop-ups on your computer. Adware can be legitimate software, but is often installed maliciously without the consent of the end-user. This software can slow down your computer and internet browsing experience.

**ASP:** *Application Service Provider*, a third-party company that manages and distributes software-based services and solutions to their customers over a wide-area network, usually the Internet.

**BDR:** *Backup and Disaster Recovery Server*, a hardware appliance physically housed at the client's office. This "server" takes "snapshot" backups of the office servers as often as every 15 minutes and sends a copy of these backups offsite every day. These backups are image-based and can be used to perform a bare-metal restore to get your network up and running fast.

**Blackberry Enterprise Server (BES):** a software and service that connects to messaging and collaboration software (Microsoft Exchange, Lotus Domino, Novell GroupWise) on enterprise networks and redirects emails and synchronizes contacts and calendaring information between servers, workstations and BlackBerry mobile devices. Newer Blackberry devices aren't relying as heavily on Blackberry Enterprise Servers and are now offering "active sync" to communicate directly with Microsoft Exchange.

**Browser Hijacker:** malicious software that changes your default homepage and search engine without your permission.

**BYOD:** *Bring Your Own Device*, the concept of using non-company-owned assets to access a company-owned resource. An example of this would be end-users accessing a corporate network via personal tablets or smart phones. Security is a major concern where BYOD is allowed (see MDM).

**Cloud Computing:** internet based computing, whereby shared resources, software, and information are provided to computers and other devices on demand, as with the electricity grid.

**Content Filtering:** software that prevents users from accessing objectionable content via your network. Although this usually refers to Web content, some programs also screen inbound and outbound e-mails for offensive information. This software is not designed for virus, worm, or hacker prevention.

**Cookie:** a file placed on your computer to allow websites to remember something. Originally designed to be helpful, cookies can save and share information such as your purchasing habits, your location, and even your identity. Cookies aren't actually capable of damaging your computer, but they can compromise your identity.

**CPU:** *Central Processing Unit*, the brains of a computer.

**DHCP:** *Dynamic Host Configuration Protocol*, a method for dynamically assigning IP addresses to devices on request, rather than explicitly programming an IP address into each device. If you have a server on your network, configuring that server as a DHCP server will make it much easier to add or reconfigure individual workstations on the network.

**Default Gateway:** in a TCP/IP network, this is the gateway that computers on that network use to send data to, and receive it from, computers and networks outside of the local network. Typically, this is the router or firewall that connects the local network to the public Internet, although it might also be a router that connects to another remote server or computer within the same company.

**DMZ:** *Demilitarized Zone*, a separate area of your network that is isolated from both the Internet and your protected internal network. A DMZ is usually created by your firewall to provide a location for devices such as Web servers that you want to be accessible from the public Internet.

**DNS:** *Domain Name System* (or *Server*), an Internet service that translates domain names into IP addresses. Even though most domain

names are alphabetic, hardware devices (like your PC) can only send data to a specific IP address. When you type www.microsoft.com into your Web browser, or send an e-mail message to someone@business.com, your Web browser and e-mail server have to be able to look up the IP address that corresponds to the microsoft.com Web server, or to the mail server that receives e-mail for business.com. DNS is the mechanism for doing this lookup.

**DSL:** *Digital Subscriber Line*, a high-speed Internet service delivered over a telephone line. Compared to newer services, DSL is usually considered to be a slower technology.

**Firewall:** a device or software program designed to protect your network from unauthorized access over the Internet. It prevents traffic from coming into your network unless that traffic was requested by an internal source. It may also provide Network Address Translation (NAT) and Virtual Private Network (VPN) functionality.

**Fractional T-1:** one or more channels of a T-1 service. A complete T-1 carrier contains 24 channels, each of which provides 64 Kbps. Most phone companies also sell fractional T-1 lines, which provide less bandwidth but are less expensive. See T-1.

**Google AdWords:** Google's online advertising program. Through this program, a company pays Google to advertise their products or services when users search Google for specific keywords.

**Hosted Applications (i.e. Hosted Sharepoint or Hosted Exchange):** a service whereby a provider makes a software (e.g. email) and space available on a server so its clients can host their data on that server.

**IP Address:** an identifier for a computer or device on a TCP/IP network. The format for an IP address is a 32-bit numeric address separated by periods (IPv4)(example: 207.46.20.60). Within an isolated network, you can assign an IP address at random, as long as each IP address on that network is unique. However, if you are connecting a network or computer to the Internet, you must have a registered IP address to avoid duplicates.

**Lync:** formerly known as Microsoft Office Communicator, Lync is Microsoft's secure instant messaging client. Lync is available as part of Microsoft's Cloud offering (Office 365) and includes instant messaging and video chat.

**Malware:** a generic term used to describe various malicious software such as viruses, Trojans, spyware, and worms.

**MDM:** *Mobile Device Management*, the series of processes and programs used to control portable devices (e.g. laptops, smart phones, tablets, etc.) which access company-owned resources. MDM usually consists of policies which govern end-users and at least one application installed on the portable device which can be used to locate or erase a lost device.

**Office 365:** Microsoft's cloud service that provides a combination of hosted email (Exchange), online document collaboration (Sharepoint), and secure instant messaging and video (Lync).

**POP3:** *Post Office Protocol 3*, a method of communication between an e-mail server and an e-mail client. In most cases, when the client software connects to a POP3 server, the e-mail messages are downloaded to the client and are no longer available on the server.

**Protocol:** an agreed format for transmitting data between two devices.

**SEO:** *Search Engine Optimization*, the ongoing process or configuring a website or webpage to increase traffic directed by internet search portals.

**Sharepoint:** a document collaboration program from Microsoft that may be installed and used "on premise" or hosted in the cloud as part of Microsoft's Office 365 Suite. Sharepoint allows for secure communication among a team or workgroup.

**Spam:** unsolicited email that comes to your inbox (i.e. junk mail). Spam is often used to distribute various types of malware.

**Spyware:** malicious software that allows a third-party to gather confidential information from your computer without your permission.

**T-1:** a dedicated digital transmission line that sends and receives data at a rate of 1.544 Mbps. T-1 lines can be used to carry voice traffic, data traffic, or a combination of both. In years past, T-1 lines were considered very fast. However, with the increase in hosted services and online data, T-1 lines are often too slow for most offices.

**TCP/IP:** *Transmission Control Protocol/Internet Protocol*, the basic language that governs traffic on the global Internet, as well as on most private networks.

**Trojan:** a program that appears to be legitimate but is actually a harmful program. For example, many of today's free game downloads on the internet are actually Trojans which can damage or destroy the data on your computer.

**URL:** *Uniform Resource Locator*, the global address of documents, Websites, and other resources on the Web.

**Virus:** a malicious program that spreads by replicating itself. Viruses can spread from computer-to-computer or network-to-network. Viruses can give control of your computer to a hacker or even damage/destroy data.

**VoIP:** *Voice-Over-Internet-Protocol*, a category of hardware and software that allows you to use the Internet to make phone calls and send faxes. This technology is becoming very popular with businesses and home users alike because it can greatly reduce telephone costs.

**VPN:** *Virtual Private Network*, a network constructed by using public wires (the Internet) to connect nodes (usually computers and servers). A VPN uses encryption and other security mechanisms to ensure that only authorized users can access the network and the data it holds. This allows businesses to connect to other servers and computers located in remote offices, from home, or while traveling, in a secure manner.

## ***An Invitation to the Reader***

The reason I published this book was to fortify firm administrators with the basic knowledge they need to make a great decision when choosing an IT service company. I believe a qualified service company can contribute to your business's success just like a great marketing consultant, attorney, accountant, or financial advisor.

The technology industry is so new, and growing at such a rapid pace, that most firm administrators can't keep up with all the latest gadgets, alphabet soup acronyms, and choices available to them. Plus, many of the "latest and greatest" technological developments have a shelf life of six months before they become completely out-of-date. Sorting through this rapidly-moving mess of information to formulate an intelligent plan for growing a business requires a professional who not only understands technology and how it works, but also understands how people and businesses need to work with technology for progress.

Unfortunately, the complexity of technology makes it easy for a business owner to fall victim to an incompetent or dishonest IT service company. When this happens, it creates feelings of mistrust toward all technology consultants and vendors, which makes it difficult for those of us striving to deliver exceptional value and service to our clients.

Therefore, my purpose is to not only give you the information you need to find an honest, competent IT service company, but in doing so, to raise the standards and quality of services for all the consultants in our industry. I believe that, the more this topic is discussed, the better it will become for all involved.

I certainly want your feedback on the ideas in this book. If you try the strategies I've outlined and they work, please send me your story. If you've had a bad experience with an IT service company, I want to hear those horror stories as well. If you have additional tips and insights that we haven't considered, please share them with me. I might even use them in a future book!

Again, the more aware you are of what it takes to find and hire great consultants in every aspect of your business—not just technology—the

stronger your business will become. I am truly passionate about building an organization that delivers uncommon service to our customers. I want to help firm administrators see the true competitive advantages technology can deliver to their business, and not just view it as an expensive necessity and source of problems.

Your contributions, thoughts, and stories pertaining to my goal will make it possible. Please write, call, or e-mail me with your ideas.

