A BUSINESS OWNER'S GUIDE

FOR GROWING YOUR BUSINESS BY NOT LETTING YOUR IT OR IT SUPPORT HOLD YOU BACK

MICHAEL J. SERVIDIO

Hassle-Free IT Support

The small-business owner's guide to finding a professional, competent, honest, considerate, on-time, fairly priced and dependable IT consultant. Read this book and you'll discover:

- The REAL cost of hiring a bad IT company or person.
- The various types of technical support contracts you'll be presented, and the pros and cons of each.
- What you should expect to pay for IT services inVermont
- 21 critical questions to ask your next IT company to make sure their policies, procedures and protocols won't leave you stranded.
- Everything you need to know about contracts, payment schedules and rate negotiations.
- The scary truth about cybercrime and what you should be doing now to protect yourself.

Master Technology Strategist for Technology Consultants, Inc.: Michael J. Servidio

author of
A Business Owner's Guide For Growing Your Business By Not Letting Your IT Or IT Support Hold You Back

Michael J. Servidio
Technology Consultants, Inc.
589 Avenue D., Suite 30
Williston, VT 05495
802-865-4409
www.TCiVT.net

Helping Small-Business Owners Eliminate
Technology Headaches Finally And Forever

Printed in the USA.

Publisher: Michael J. Servidio

589 Avenue D., Suite 30, Williston, VT 05495

For Group Purchasing, Call: (802) 865-4409

www.tcivt.net

I dedicate this book to Marian my Wife;
she has been an inspiration to keep working hard to be a better person.

CONTENTS

Introduction

IT: A Necessary Evil?

There are very few businesses that can operate without some dependence on technology.

From e-mail, phone systems and websites to CRM software, accounting applications, HR management and industry-specific line-of-business applications, we've eliminated a lot of manual labor and paper using high tech – and that's a good thing.

Used correctly, technology can secure faster production, increased productivity, more sales, superior customer service, marketing multiplication and up-to-the-minute business intelligence you can't get with paper and ink or old-fashioned, nontech systems. But nothing in business is "all good," including tech.

But Increased Productivity And Automation Come With A Cost

The downside of this vast dependence on technology is that when it doesn't work, it can become a tremendous source of frustration, putting a major strain (or a complete halt) on production, sales and fulfillment. No business is immune to technical problems and IT failures, and it can often feel like every time you turn around, something is down, not working and in need of MORE money to make it work.

Then there's the complexity of it all. Installing and supporting even a small network requires specialized knowledge and skills that most small-business owners don't have in-house.

Many applications don't work with each other, so you need to hire (expensive) specialists to install, set up and configure your applications and developers to write "bridges" to get one application to talk to another – a never-ending cycle of spend, spend, spend.

And let's not forget about the growing tsunami of cybercrime and ransomware. The equivalent of modern-day train robbers, international hacking groups have discovered that it's incredibly easy to target businesses like yours because you simply don't have the budget to spend on IT security like larger organizations do. You're low-hanging fruit. Sure, they might not get $10 million from you, but they might get $10,000 or $100,000; and since there are far more small businesses out there than large corporations, many hackers focus on the easy money found in the millions of small businesses like yours.

Why You Need This Book

If a large corporation makes a $50,000 technology mistake, it's certainly not a good thing, but it represents only 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, not to mention the interruption to their business and the distraction it can create. That's why you have to be extra careful in who you take IT advice from and why we wrote this book.

Very few business owners are technically savvy enough to know if the advice they are being given is correct or if the fees they're paying are fair and reasonable. When you're not technical, you are forced into a position where you must trust the person giving the advice – and the most expensive advice is bad advice.

Once you find a competent, trustworthy IT consultant, you can free up your time and attention to running your business and activities that drive sales and profitability. They can make your life easier and give you peace of mind that you're protected and secure from a devastating ransomware attack or data breach. And the right consultant thinks like an entrepreneur, not a tech, ensuring that

whatever you implement will support the productivity and profitability of your business now and over the long haul, giving you the best possible return for your IT investments. To that end, this book will give you:

- The right questions to ask any IT person or company BEFORE you sign a contract. This is really, really important because you are handing over the "keys to the kingdom" to your IT person or company, and you need to know they will handle that responsibility ethically, honestly and reliably, not hold you hostage and take advantage of you.
- How to avoid wasting money on unnecessary "latest and greatest" technology, fads and "cool toys" that don't deliver an ROI for you AND how to avoid overpaying for IT services.
- What you need to know in order to make sure your data and your company are protected from an ever-growing list of threats, including ransomware, hackers, faulty hardware and software and even employee sabotage.
- If you have remote staff, how to make sure your employees are actually WORKING when remote and NOT doing things that could jeopardize the security of your business and tank productivity.
- What you need to do to stay up-to-date and ahead of compliance regulations that require you to protect your clients', patients' and employees' data. Claiming ignorance is not an acceptable defense if your network gets compromised and the regulators get involved. Fines and penalties can be levied on you even if you trusted your IT person or company to ensure you were compliant.

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

Chapter 1:
Four Decades Of No-Fuss IT Support

From Handwriting To Hardware

Back in the early 1980s, I was working with my brother, a structural engineer. He had no patience for my handwriting, and honestly, I can't blame him. That frustration turned into opportunity. We started exploring computer-aided design, or CAD, as a solution long before it became mainstream. In fact, we were among the first in Vermont to use a desktop version of AutoCAD.

At the time, there weren't many people using personal computers for business. But we were, and pretty soon other professionals started asking us, "How are you doing that?" They wanted to know how this emerging tech could fit into their work. That's when I realized there was a need for someone who could bridge the gap between technology and real-world business needs.

The introduction of personal computers allowed users to type out documents, and some models included spreadsheets for making informed accounting decisions. You could go to a local store and purchase a computer. It had very little ability, but it was better than using an electric typewriter. But the dilemma was what to get and when to purchase one, what other items would you need? The salespeople did not have a full understanding of what a small to medium business would need or even want for their job. We will talk more about that later.

In 1986, I launched my own company, then called Computer Technology Consultants. At first, it was just me helping businesses understand and integrate this new thing called a personal computer. Most people didn't know what to buy,

let alone how to use it. I didn't sell hardware. I gave them the know-how and confidence to use the tools that could transform their business. I began by helping them put together a list of items they would need, and then going to the different computer stores to gather prices and comparisons of each. That is what people really wanted.

My background in construction and engineering gave me a practical mindset. I didn't come from a tech lab. I came from job sites and business offices where people needed solutions that worked, not theory. That hands-on experience laid the foundation for everything we do now. The tools have changed, but our approach remains the same. We figure out what the client really needs, then make the technology do the work.

That's how it started; Not with a grand vision, but with a problem, a little ingenuity, and a willingness to help. And it's why, nearly forty years later, we're still doing exactly that.

Who We Serve And Why

When I first started, we focused heavily on architects and engineers because that's the world I came from. We provided CAD support, system setups, and consulting that helped design professionals modernize their workflows. But in 1991, everything changed. The Gulf War hit, and business in that sector dried up almost overnight. That was a wake-up call.

I realized I couldn't put all my eggs in one basket. Specializing too narrowly nearly cost me everything. So, I pivoted. I opened up my services to general businesses, really anyone who needed a computer. That decision didn't just save my company. It gave me long-term resilience.

In the last decade or so, we've found a new sweet spot—private healthcare practices, dental offices, and law firms. These aren't just random industries we happened to land in. They're professional fields where data protection, compliance,

and system reliability matter a great deal. And they're led by people who don't have time to deal with IT headaches.

A key turning point was when I began working with the Vermont Bar Association. That relationship led to deeper involvement with law firms across the state, and we built up a strong reputation for understanding their specific needs. Document security, reliable remote access, and compliance are all critical in that field.

Dental practices and private medical offices followed a similar pattern. They needed someone who understood not just the tech, but also the flow of a busy office, the quirks of specialized software, and the stakes of even an hour of downtime. That's where we came in. We didn't just fix computers. We made sure they could focus on their patients and clients without worrying about the backend.

Today, we continue to support a variety of small businesses, but law, dental, and healthcare comprise the bulk of our focus. We know their systems, their pace, and their pain points. We provide calm, clear solutions that keep things running smoothly.

When Technology Just Doesn't Work

If I had to sum up most of the problems new clients bring to us, it would be this: "It's not working, and I don't know why."

That simple phrase shows up in nearly every first call. Sometimes it's a server issue. Sometimes it's a string of frustrating glitches. Often, it's just confusion. A small business owner might be staring at a screen that won't load, wondering why their printer isn't printing or why their email keeps bouncing back. And when you're trying to run a business, you don't have time to diagnose the problem. You want it fixed.

Many of our clients come to us after working with another IT company. In some cases, they're frustrated because things were never properly explained to them. In others, they were handed over to multiple people who didn't take the time to understand the business. By the time they reach us, they're overwhelmed and often a little skeptical. They've been burned before.

One of the most common underlying issues is overcomplicated setups or poorly managed handoffs. When we do our first review, we often find systems that were patched together over time without a clear strategy. Or we find technology that was set up but never really explained. That's where we come in. Not to point fingers, but to clean up the mess and bring clarity.

We don't blame the other guy. That's not our style. In fact, we've even had competitors call us for help, and we've gladly given it, quietly and without credit. That's because our job is to solve the problem, not make someone else look bad. We understand that at times our IT competitor would recommend changes to their client, but due to some Geek Speak, the client did not understand what or why the change would be needed, and thus did not do it—and later paid the price. We have had to help get the information to the client, so they understand what was being asked of them. At times, our colleagues (our competitors) would be able to keep the client and are still working with them even today.

In the end, most of the issues we deal with boil down to one thing. The client doesn't want to have to think about the tech. They just want it to work. And that's exactly what we aim to deliver.

Why The Right IT Partner Matters

Technology isn't just equipment; it's the foundation that keeps your business running, quietly and consistently in the background. What was once merely an added piece of equipment for convenience is now required to get the job done. When that foundation cracks, the ripple effects can bring your whole operation to a standstill. That's why having the right IT partner isn't a luxury; it's a necessity.

Over the years, I've seen the damage caused by poor IT support. I have seen good-meaning IT support that has not received the necessary training or in-depth support from manufacturers that partner with IT firms, and thus the client has lost time, data, and trust. Not because the previous provider was malicious. Often, they simply didn't understand the client's business well enough, or the need for a true business-class product. They set things up by the book but missed the real-world details that make all the difference. Or worse, they overcomplicated everything, leaving the client afraid to touch anything.

We work differently. Our job is to make tech invisible. We create systems so well-tuned that our clients barely notice they're there. That means being proactive. We don't wait for something to break. We look for the warning signs before it becomes a fire drill. We train staff. We check in. We take ownership of the systems, even when the problem isn't ours. When something does go wrong, we don't pass the buck. If it's a printer problem, a software glitch, or an internet outage, we help solve it, even if it means dealing with a third-party vendor on the client's behalf. That's what people remember. Not only did we fix the issue, but they also didn't have to chase five different people to get it done.

The impact of solid IT support is hard to measure until you've gone without it. Our clients often tell us the biggest benefit is peace of mind. They can focus on running their business, knowing we're in their corner. That kind of trust takes time to earn. However, once we have it, it becomes the strongest part of the partnership.

Practical IT That Just Works

Our approach has always been simple. Solve the problem. No finger pointing, no jargon, no endless back-and-forth. Just get it working so the client can get back to business. That mindset comes from years of hands-on experience. I didn't learn IT in a classroom. I learned it by sitting with clients, rolling up my sleeves, and figuring things out alongside them. That foundation taught me to see the big picture. It's not just about fixing a single machine. It's about ensuring the entire system supports how the business operates.

Clients don't need complicated setups. They need reliability. They need someone who understands that tech is a tool, not a showpiece. If we can reduce clicks, simplify workflows, or automate a manual process, that's a win. We're not here to impress people with specs. We're here to make life easier for the person sitting at the desk.

Sometimes the fix is technical. Other times, it's administrative. I tell people all the time that technology is only part of the equation. Policies, habits, and human error often cause more trouble than the hardware ever will. We help with all of it because if it affects how the system runs, it's our job to step in.

Over the years, we've developed a reputation for being the team that owns the problem. Even if the issue is with another vendor or a third-party product, we don't pass it off. We take responsibility, coordinate the solution, and follow through until it's resolved. That's what clients remember. That's why they stay.

When people say they appreciate that we make it so they don't have to think about IT, I take that as the highest compliment. That's the goal: quiet systems, smooth days, and the freedom to focus on what matters most.

Helping Small Businesses Scale

One of the most satisfying parts of this work is watching a small business grow into something remarkable. Over the years, we've seen it happen again and again. A husband-and-wife team working from a home office. A start-up with three employees and a big idea. A local shop trying to modernize their systems. These are the businesses we support, and many of them have become major players in their industries.

One client started after leaving a large construction firm. He and his wife decided to go out on their own and asked for our help setting up their IT infrastructure. They didn't have much at the time, just a few computers and a vision. Today, that company brings in over 45 million dollars in revenue and is one of the largest construction firms in Vermont. Eventually, they outgrew us and

hired their own internal IT team. But the owner still calls from time to time, just to say thanks. He credits those early tech decisions as a key part of their growth.

Another client is now the largest maple producer in the United States. When they started, they had no digital systems in place. We helped them implement everything from basic email to full-scale operations management. Within three years, they became the industry leader. We're still with them today, and it's been rewarding to see that kind of progress up close.

But it's not always about massive growth. Many of our clients are happy to go from a two-person shop to a team of 20 or 50. That kind of success is just as meaningful. They become more efficient, more profitable, and less stressed. And we know we played a role in that.

What we do isn't flashy. But it's foundational. Good IT gives businesses the ability to grow with confidence, knowing their systems won't hold them back. That's what we offer. Steady, reliable support that scales with your vision.

Our Secret Sauce: Just Be Human

If there's one thing that truly sets us apart, it's this. We treat people like people. It sounds simple, but in the world of IT, it's surprisingly rare.

We don't just talk to decision-makers. We make it a point to connect with everyone in the business, from the CEO to the janitor. That's not a strategy. It's just who we are. And it's one of the things clients appreciate most. Over and over, we hear that they feel seen, heard, and respected. That matters more than most people realize.

I teach my staff (colleagues) the same mindset. Treat everyone kindly. Listen. Be patient. You never know who your next boss might be, and more importantly, everyone's role in the business is important. Whether they're answering phones or running payroll, they deserve respect and support. That attitude builds trust fast, and it lasts.

Clients also come to trust us with more than just their tech issues. Sometimes we receive the call when they're dealing with something personal or sensitive, like parting ways with a business partner or preparing to restructure. That level of trust doesn't come from fixing a printer. It comes from being consistent, honest, and approachable.

We don't claim to have all the answers, and if someone says they do, well I would say do not deal with them. But we do promise to care, to show up, and to figure things out without drama. We don't talk down to clients or bombard them with jargon, what we call 'geekspeak.' We explain things clearly, solve problems quietly, and move on.

That might not sound revolutionary, but it is. In a world full of outsourced call centers and finger-pointing service providers, just being human goes a long way. It's what makes us different. And it's why so many clients have stayed with us for decades.

Where To Start If You're Stuck

When a business is overwhelmed by IT issues, the biggest challenge isn't always technology. It's knowing where to begin. That's where we come in. We help clients take a breath, step back, and look at the big picture.

The first step is almost always clarity. What systems are in place? What's working? What's not? You'd be surprised how many businesses are running on outdated or unnecessary tools simply because no one has had time to stop and assess. We help clients identify the pain points and prioritize what matters most.

Next, we look for quick wins. Sometimes it's as simple as reorganizing file structures, adding a backup solution, or implementing a basic password manager. These are low-hanging fruit that can immediately reduce risk and improve workflow without a big investment. It's not about doing everything at once. It's about taking smart, manageable steps in the right direction.

We also help businesses understand the importance of policies and processes. That might mean setting standards for how data is stored, when passwords should be changed, or how updates are handled. These administrative tweaks often have more impact than a new piece of hardware.

For owners who feel stuck, my advice is to find someone you trust, who has testimonials, or someone who has the certifications to do an honest assessment. This may not be and should not be someone who is a friend or relative who seems to be a wiz at computers. You need someone who has experience. Not a hard sell, but an honest conversation about what's holding you back and how to move forward. IT doesn't have to be intimidating. With the proper support, it becomes a quiet strength in the background of your business.

You don't need to be an expert to run a tech-savvy business. You just need the right partner to guide the way. That first call is often the turning point.

Supporting Growth, Then Stepping Back

One of the best parts of this work is seeing clients grow. We've helped businesses go from a couple of desktops to multi-million-dollar operations. Some outgrow us, build their own internal IT teams, and move on. And that's a win in my book. It means we did our job right.

We don't hang on just to keep a client. If they've grown to the point where they need something different, we support that. We stay available, we cheer them on, and sometimes, they still reach out for advice. It's a sign of mutual respect and trust that's been built over years.

I take pride in knowing that the work we do behind the scenes has helped real people succeed. We've made their days easier, helped them avoid crises, and in some cases, freed them up to go home a little earlier to their families. That matters. It's not just about machines and servers. It's about the people using them and the businesses they're trying to build.

As I look back on four decades in this field, one thing is clear. Technology will always change, but the need for clear, steady support will not. Business owners want someone who will listen, explain, and follow through. That's what we've built our reputation on.

To the reader: if your IT feels like a mess, or you're just tired of worrying about what could go wrong, know that it doesn't have to be that way. There are honest, reliable partners out there who can help you build something strong. Whether you're just starting or scaling fast, the right tech support can make all the difference.

Keep reading. There's a lot of wisdom in these pages. And if our story sounds familiar, maybe it's time to write the next chapter for your business too.

Chapter 2:
The True Cost Of Bad Advice And Poor IT Support

Let me tell you a true story about "Bob."

No one is exempt from IT problems. While all business owners can relate to the sheer frustration these issues create, few can put a dollar figure to the actual hard cost to their business when IT problems occur. That's because so many of these issues happen randomly and can be difficult to measure.

However, no business owner can deny that IT problems cost money. If you've ever had your day grind to a screeching halt because the Internet went down, e-mail stopped working or some IT system suddenly "broke," you know everyone stops doing productive work to try and replace the "flat tire." In today's microwave deadline world, that's not good.

Plus, technology should work. You shouldn't feel like every day is a whack-a-mole game to troubleshoot the IT problem of the day or to keep putting out fires that reoccur. If you do, then I can assure you it's costing your business money – and you have the wrong IT person or company working for you.

But how much money do these constant IT "glitches" cost? It's hard to tell exactly because there is a large degree of variance based on the characteristics of your business and the specific problems you're having. So, let's take a look at these statistics on the cost of IT-related downtime and disasters, as reported by various industry experts and studies:

- The average cost of IT downtime is $5,600 per minute. This may sound like a lot, but when you factor in salespeople who cannot sell or an entire department being unable to work, book appointments and process orders, it's not hard to get to that metric quickly. (Source: The Cost of Downtime, Gartner)
- 93% of companies that lost their data center for 10 days or more due to a disaster (natural or ransomware) filed for bankruptcy within one year of the disaster, and 50% filed for bankruptcy immediately. (Source: National Archives & Records Administration in Washington)
- The National Cyber Security Alliance reports a whopping **60% of companies close their doors permanently** within six months of falling victim to a data breach.
- According to CNBC, hackers targeted small businesses 43% of the time.
- **The average total cost of recovery from a ransomware attack has more than doubled in a year, with the average ransom paid of $170,404.** Further, only 8% of the companies paying a ransom get all their data back. (Sophos, "The State of Ransomware 2021")
- Cybercriminals **stole an average of $900 from 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 from an inability to work, there IS a cost to you and your team when you're constantly aggravated and frustrated because you can't work.

If your sales department can't make calls or your operations team can't deliver on contracts, that's a MAJOR source of frustration for everyone – including clients who are impacted by delays. It hurts morale, sales and customer relationships ("Sorry, Charlie, I can't help you because our systems are down…again"). Worst of all, it's 100% unacceptable and preventable.

The Cost Of Bad Advice

In addition to downtime and broken systems, there is another cost that most business owners don't consider: **the cost of bad advice when an inexperienced or unethical consultant recommends a product, service or project that is unnecessary or incorrect for your specific situation.**

Sometimes bad advice is due to sheer ignorance and inexperience. Sometimes it's because the IT company is knowingly trying to keep the price down (so you'll say yes and buy from them), recommending a substandard product or solution just to get the sale. Sometimes they're selling you top-of-the-line solutions but installing cheap products and shortcuts to pad their bottom line.

Very often, IT companies and technicians choose simple solutions they are familiar with and can easily manage instead of the best solution for the problem, which may require expertise they don't have or additional setup, support and maintenance they don't want to do.

For example, we could lock your front door with standard locks, and it would work to keep some people out – but not an experienced, determined criminal. A better solution would be dead bolts and a home security system that is complete with motion detectors, cameras and glass-break technology. Setting that up requires more work, and your home needs to be monitored, but if you want to make sure no one breaks in when your family is sleeping or while you're away on vacation, that's the type of system you need.

Another form of bad advice is when an IT consultant lacks experience in solving a problem, grossly underestimating the time and money it will take to successfully complete a project. When a consultant makes this mistake, your project ends up way over schedule, costing you two to three times as much in unexpected fees to get it done. Believe it or not, a lot of IT people are NOT very good at planning.

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."**

Here's a list of other ways bad IT advice can cost you:

- You can end up paying for unnecessary services, software, hardware and consulting fees and STILL not get the solution or results you wanted.
- You can pay for IT maintenance but still be left wide open to a ransomware attack, with no means for getting your data back except by paying the ransom and hoping you get your data back.
- The above will also cost you THOUSANDS in emergency data restoration services. You cannot just "unlock" your data. Someone has to comb through your files and devices to ensure the hackers haven't planted another virus to ransom your network again in the future (after all, you've demonstrated you're a paying customer). You might need to rebuild your network from a backup, which can take weeks. Don't underestimate the devastating costs and losses from one attack!
- Handling the public relations nightmare of your clients' data being exposed via a breach and having to notify your clients that you exposed their personal data, medical files, credit cards, e-mail, etc., to hackers.
- Compliance and data breach violations and fines. Every state is instituting stronger rules about what every business – from a solo entrepreneur to a major corporation – must have in place to protect private information; and private information isn't just medical records and financial data, but also e-mail addresses, birthdays, social security numbers, mailing addresses, phone numbers and more. Neglect to put proper protections in place and you could end up being slapped with fines and legal fees to defend yourself.
- Getting stuck with a "solution" that doesn't really solve your problems, wasting time and money, forcing you to start over, again.

- Paying double by having a competent IT consultant fix what the other person messed up or complete the project you originally wanted done (and paid for).
- Throwing away all the time and money you put into a project you've paid big money for because the solution was too complicated to actually use and employees either couldn't use it or refused to use it (this happens with custom development all of the time).
- Incurring litigation costs to get your money back from a technician who ripped you off or failed to deliver on a contracted service.
- Dealing with the sheer frustration of the problems resulting from poor advice.

The trouble is, it's hard to know when you're paying for bad advice until you are already neck-deep in the problems and it's too late. By the time you suspect that you've hired the wrong person, 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.

Worse yet, IF you do get breached, you'll be scrambling to find someone else to help you put all the pieces back together again, forced to make another quick decision on who to trust under pressure and having to throw more money at someone, hoping they'll do the right thing.

That's why the information in this book is so critical. Your best defense against this painful, expensive, business-interrupting nightmare is to become an educated consumer who does their homework before they make the wrong decision.

Chapter 3:
10 Common Mistakes To Avoid When Choosing Your Next IT Consultant

Just like every industry, the IT industry has its fair share of unethical, incompetent and inexperienced practitioners who survive only because most business owners aren't technical and can't know, for certain, if the work they're doing and the recommendations they're making are incorrect, incomplete, insufficient or flat-out *wrong*.

Just start asking some of your business colleagues about "bad" IT mistakes and you'll get an earful of the horror stories and disappointing experiences they have encountered in this area.

From misleading information to 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. Sometimes this is out of greed for your money, but more often it's simply because they don't have the technical expertise, staff and experience to do the job right, but won't tell you that up front.

To make matters worse, **the IT industry is not regulated like many other professional service industries**, which means ANYONE can claim they are an "IT expert" or "cyber security specialist." 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. That means many of the so-called experts are useless and make the sleazy auto repair shops look like the pinnacle of virtue and competence.

Automotive mechanics, 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 technology industry is still highly unregulated and there aren't any laws in existence to protect you, the consumer.

Can you imagine anyone being able to hang a shingle out and claim to be an accountant or doctor without specialized training and a license to practice? Would you want that person treating your illness or handling your tax return? Or an attorney who never went to law school nor passed the bar exam? Even truck drivers need training and a license to operate. But, unfortunately, that's how the IT industry works, and anyone can claim to be an IT expert, even if they don't have training, certifications or experience.

That's why it's SO important for you to do your due diligence and use this book to weed out the incompetent charlatans. Here are 10 mistakes to avoid when you're conducting that search:

- **Mistake #1: Choosing your next IT person or company based purely on price.** We all know you get what you pay for, and the last place you want to be cheap is when it comes to IT security, data backups and disaster recovery of data. What you save in services fees you'll end up paying for in problems

  That's not to say the highest-priced IT person is the best either; larger IT firms may be more expensive simply because they have more overhead and may use higher prices to weed out small businesses with smaller IT budgets. If you're a small business (under 100 employees), they might not really want you either, giving their best techs and services to larger organizations with bigger budgets.

Choose your IT company based on reviews and competence and the answers they provide to the questions later on in this book, not just on the prices they charge.

- **Mistake #2: Choosing an IT company based on their marketing claims.** While good marketing is not necessarily a bad thing, the sad truth is that all IT companies will tell you they're responsive and proactive and they care about building relationships with you. (Gee, wouldn't you expect your IT company to care about you?)

  Most IT marketing gives you very little information upon which you can make a good decision, so don't just rely on slick marketing materials – do your due diligence as outlined in this book and ask the tough questions we've provided you. You'll be able to cut through any marketing B.S. and see if they can and will do the job you need.

- **Mistake #3: Choosing your next IT company based solely on a referral.** Of course, referrals are the lifeblood of any good IT firm, but make sure the person who is referring you actually knows how to pick a good IT firm and their own IT needs are similar to or more complex than yours.

  We're all busy, so it's tempting to get a little lazy when you are referred to a company by someone you trust. It's tempting to forgo your normal research and not look at competitive bids, ask the tough questions, etc. My advice is that you should still ask the tough questions and conduct some due diligence.

- **Mistake #4: Falling for signing a long-term contract.** How can you be asked to sign a two-year or three-year contract when you've never done a single project with them? This is a big red flag. Make sure you can get out of that contract easily if they fail to deliver the level of service you deserve. In my IT business, we had a one-year contract and outlined in our Master Service Agreement along with any Satement of Work what we are to provide and if we fail at providing that server they can cancel our contract.

- **Mistake #5: Hiring them before you've spoken directly with three to five of their long-term current clients who have a business similar to yours.** Don't let them give you just any client to talk to. Make sure you talk to clients who are similar in size, employees, locations and technology. If you have a particular project in mind, ask to speak to another client for whom they did a similar project.

  Another good sign is that they have multiple client reviews online and success stories posted on their website and on review sites like Google My Business. A lack of this may be a sign that they don't have clients who are happy enough to provide a good reference. While I wouldn't completely dismiss a company based on a low number of positive reviews, I do suggest you at least look to see if they have any, and if any are negative.

- **Mistake #6: Hiring an IT company that doesn't insist on doing a network assessment of some kind BEFORE they provide you a quote or recommend an action plan.** Any competent professional should offer to do an audit or assessment to diagnose your situation BEFORE quoting you anything. 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.

  Remember, how they interact with you initially in the sales process is a very good indicator of how they will work with you after you hand over your money. GOOD diagnostics and researching a problem are always necessary for recommending the right plan of action. I'd be very nervous if the company I was looking to hire didn't insist on doing that initial deep dive into our computer network before they start proposing "solutions" (selling).

- **Mistake #7: Hiring an IT consultant who isn't very experienced with (and recommending) a cloud option.** Many inexperienced consultants are only knowledgeable about how computer networks were designed ten years ago, when physical servers and equipment inside your office was the only option (or a better option). While there is certainly still a place for physical servers and devices, newer cloud technologies such as Microsoft 365, Amazon Web

Services and Microsoft Azure are often capable of providing the same or even better solutions at a lesser cost and with more flexibility and security. A great consultant will know these technologies and offer them as an option (either fully cloud-based or a hybrid solution of cloud and on-premise hardware). A really great consultant will be able to figure out what provides the best return on investment for you and what's in alignment with the longer-term goals and work preferences of your business. Further, many technologies are moving in the direction of cloud-based solutions, so you might find your IT company completely out of touch and unable to provide support when cloud-based is the only option for some applications.

- **Mistake #8: Don't hire a consultant who can't (or won't) remotely monitor your computer network via "managed services."** With cyberthreats at an all-time high and businesses relying on uptime, you'd be a fool not to have someone monitoring and maintaining your network, security and backups on a daily basis. IT consultants who can't or won't do this are dinosaurs living in the Stone Age and are NOT doing you a favor or "saving you money."
- **Mistake #9: Never hire an IT company that doesn't make cyber security one of their TOP priorities.** The old saying that the cobbler's children never have shoes is never an acceptable excuse for an IT company having lax security measures. If they get hacked, YOU'LL get hacked. Be sure to ask the questions we've outlined in the next chapter specific to cyber security and do NOT hire them if they seem evasive, nervous or even angry when you grill them on THEIR cyber security practices.
- **Mistake #10: Never hire a "one-man band" to handle IT for you.** If they get sick or go on vacation, you're without THE GUY (or gal) who knows all the passwords, how things are set up and how to make things work. That's VERY dangerous.

  I've heard countless stories of situations where their IT person went "missing" along with the keys to the IT kingdom, never to be found again. Recently a friend called out of desperation because his solo IT guy was in prison (!) and unable to share passwords or relay where the backups were stored. Yes, that's

extreme, but it's not uncommon for a solo tech to be unavailable or have personal problems that prevent them from helping you. You want to hire someone with a team, and preferably a LOCAL team (not an outsourced help desk overseas) that has more than one tech who knows your network, your passwords, your systems and preferences.

Chapter 4:
23 Critical Questions That Reveal If The IT Company You're Considering Is Trustworthy And Competent

In this part of the book we're going to give you the nitty-gritty questions to ask before you sign a contract with any IT company. If at any point they become uneasy, appear to be evading your questions or dismissing and downplaying them, that's a warning sign.

How they behave now when they're trying to earn your business is a good example of how they will act after you hire them – and you should be able to ask them any question and get straightforward answers, in plain English (not geek-speak).

Further, I strongly recommend you get these terms IN WRITING in the contract. They might say they offer after hours but may have a carve-out in their agreement stating that that costs extra, or the response time isn't guaranteed in writing.

Now, here are the questions to ask, broken down by category.

Customer Service

Q1: When I have an IT problem, how do I get support?

In the IT industry, we have systems to manage your requests and IT issues. When a client has a problem, we "open a ticket" in these systems so we can properly assign, track, prioritize, resolve and document the various client issues we're working on.

However, some IT firms force you to log in to a portal to submit a ticket and won't allow you to call or e-mail them. This is for THEIR convenience, not yours. What do you do if the Internet is down or you can't log in to the portal? Trust me when I say this will become a giant inconvenience and thorn in your side. That's not to say they shouldn't offer that as an option, but it shouldn't be your ONLY option for requesting support.

Also, make sure they HAVE a system in place to keep track of client "tickets" and requests. If they don't, I can practically guarantee your requests will get overlooked, skipped and forgotten from time to time.

So, be sure to ask how you and your team can submit a problem to their support desk for resolution. Can you call them? Send an e-mail? Requesting support should be EASY for you.

Q2: Do you offer after-hours support, and if so, what is the guaranteed response time?

Any good IT company will answer their phones live and respond to your calls from 8:00 a.m. to 5:00 p.m. every day. But they should also have the ability to provide after-hours support on nights and weekends.

Many CEOs and executives work outside normal "9 to 5" hours and find it the most productive time they have. If that's true for you, make sure your IT company offers an after-hours support line with a one-hour to two-hour response time.

Q3: Do you have a written, guaranteed response time to working on resolving problems?

Most IT firms offer a 60-minute or 30-minute response time to your call for help during normal business hours. Be very wary of someone who doesn't have a guaranteed response time in writing – that's a sign that they are disorganized and/or possibly understaffed to handle your requests. A written, guaranteed response time should be standard in every service agreement you sign.

Q4: Will I be given a dedicated account manager?

Smaller firms might not offer this due to staff limitations, and the owner may tell you they will personally manage your account. That sounds like great customer service, but the owner of the company is often pulled in so many directions that you'll only get reactive support and reactive customer service instead of proactive account management.

Q5: Do you have a feedback system in place for your clients to provide "thumbs up" or "thumbs down" ratings on your service? If so, can I see those reports?

There are many applications that IT companies use to get customer feedback on the quality of service they're providing – and great IT firms want that feedback to ensure their engineers are taking great care of their clients.

If they don't have this type of system in place, be leery. If they DO have one in place, ask to see the actual scores and reporting. That will tell you a lot about the quality of service they are providing. A great IT firm with happy customers will be eager to share that information with you; someone who's not delivering great support and not getting excellent scores will hide that fact or be hesitant to share that with you.

IT Maintenance (Managed Services):

Q6: Do they offer true managed IT services and support?

As mentioned earlier, you want to find an IT company that will proactively monitor for problems and perform routine maintenance on your IT systems. If

they don't have the ability to do this, or they don't offer it, we strongly recommend you look somewhere else. If they say that they set the computer's operating system to automatically check and apply updates and you do not need to do anything more, then you should not consider that person or company. A good managed service company would have their team review and approve the updates needed before they are applied.

Q7: What is NOT included in your managed services agreement?

Another "gotcha" many IT companies fail to explain adequately is what is NOT included in your monthly managed services agreement that will trigger an invoice. Often, IT companies will tell you they offer an "all you can eat" option. That's RARELY true – there are limitations to what's included and you want to know what they are BEFORE you sign.

It's very common for projects to not be included, like a server upgrade, moving an office, adding new employees and, of course, the software and hardware you need to purchase.

But here's a question you need to ask: If you were hit with a ransomware attack, would the recovery be EXTRA or included in your contract? Recovering from a cyber-attack could take HOURS of high-level IT expertise. Who is going to eat that bill? Be sure you're clear on this before you sign an agreement, because surprising you with a big, fat IT bill is totally and completely unacceptable.

Other things to inquire about being included are:

- Do you offer truly unlimited help desk? Sometimes agreements will give you a certain number of hours and then bill you for anything over that. Make sure you aren't getting nickel-and-dimed for every call.

  Does the service include support for cloud services such as Microsoft 365?

- Do you charge extra if you have to resolve a problem with a line-of-business application, Internet service provider, phone system, leased printer, etc.? If they didn't install it, do they support it or do they bill extra for it? What you

want is an IT company that will own the problems and not point fingers. That may require them to call the vendor or software company on your behalf. Good IT companies will be happy to do that for you as part of their agreement. Others may refuse to or may bill you for the service. Clarify this up front.

- What about on-site support calls? Or support to remote offices?
- If your employees had to work remote (due to a shutdown, natural disaster, etc.), would you provide support on their home PCs or would that trigger a bill?
- If we were to get ransomed or experience some other disaster (fire, flood, theft, tornado, hurricane, etc.), would rebuilding the network be included in our service plan or considered a project that we would have to pay for? This is something you want to get IN WRITING. Recovering from a disaster such as this could take hundreds of hours of time for your IT company's techs, so you want to know in advance how a situation like this will be handled before it happens.

Q8: Is your help desk local or outsourced?

Be careful if they don't maintain and manage their own local help desk. Smaller IT firms will outsource this critical function because they don't have the ability or funds to hire their own team.

When they outsource to a third party, you may end up getting a tech who is not familiar with you, your network, previous problems and personal preferences. This can be frustrating and lead to the same problems cropping up over and over, longer resolution time for critical issues and you having to reeducate the tech on the history of your account. Ideally, look for a company that will dedicate a person and/or team to your account so they get to know you, your company, preferences and history, making them more capable of resolving problems and handling things the way you want them handled.

Q9: How many engineers do you have on staff?

Be careful about hiring small, one-person-shops or IT firms that only have one or two techs. Everyone gets sick, has emergencies, goes on vacation and needs to take a few days off from time to time; that's why you want to make sure whomever you hire has enough techs on staff to cover if one of them is unable to work.

Q10: Do you offer documentation of our network as part of the plan, and how does that work?

Network documentation is exactly what it sounds like: the practice of maintaining detailed, technical records about the assets you own (computers, devices, software, directory structure, user profiles, passwords, etc.) and how your network is set up, backed up and secured. Every IT company should provide this to you in both written (paper) and electronic form at no additional cost and update it on a quarterly basis.

Why is this important? There are several reasons:

First, it shows professionalism and integrity in protecting YOU. No IT person or company should be the only holder of the keys to the kingdom. By documenting your network assets and passwords, you have a blueprint you can give to another IT person or company to take over if necessary.

Second, good documentation allows the engineers working on your account to resolve problems faster because they don't waste time trying to fumble their way around your network trying to find things and uncover accounts, hardware, software licenses, etc. Third, if you had to restore or recover your network from a disaster, you'd have the blueprint to quickly put things back in place as they were.

And finally, and most important, if you ever find yourself in a position where you need to switch IT providers, your replacement company will be able to take over quicky because the network has been documented properly.

Side Note: If your current IT person or company refuses to do this, or has the documentation and won't share it with you, they need to be fired. This is downright unethical and dangerous to your organization, so don't tolerate it! But before you fire them, find a reputable company who can "sneak" into the network, get the necessary credentials and lock them out before they do you harm.

Q11: Do you meet with your clients quarterly as part of your managed services agreement?

Professional IT firms will offer to meet with you at least quarterly (sometimes more often) to provide a "technology review."

In this meeting, they should provide you with the status updates of projects they're working on and the health and security of your network. They should also be making recommendations for new equipment and upgrades you'll be needing soon or sometime in the future and discussing with you future plans for expansion and contraction so they can support your business goals.

Those meetings should be C-level discussions (not a geek-fest) where IT budgets are discussed, as well as critical projects, compliance issues, known problems and, of course, cyber security best practices.

They should be constantly bringing you new ways to improve operations, lower costs, increase efficiencies and ensure that the productivity of your organization stays high. This is also your opportunity to give them feedback on how they're doing and to discuss upcoming projects.

Q12: If I need or want to cancel my service with you, how does that happen and how do you off-board us?

Make sure you carefully review the cancellation clause in your agreement. Many IT firms hold their clients hostage with long-term contracts that contain hefty cancellation penalties and will sue you if you refuse to pay.

Our advice is to look for someone who will allow you to cancel and end an agreement without contention or fines. Occasionally, a longer-term agreement with cancellation penalties is justified if they are investing in hardware, software or specialized talent they need to acquire to deliver on the agreement, but those are special circumstances. Always agree in advance how you can get out of the contract before you need to trigger that clause.

Cyber Security:

Q13: Tell me about the cyber security certifications you and your in-house team have?

The Certified Information Systems Security Professional (CISSP) certification is one of the best security certifications they can have. Others include the CEH, or Certified Ethical Hacker; CISM, Certified Information Security Manager; and CompTIA Security +. Of course, there are dozens more.

While you won't be able to keep up on these certifications (much less understand them!), the key is that they have some type of recent training and certifications, and should be able to answer this question, which demonstrates a dedication to learning and keeping up on the latest cyber security protections. If they don't have any, and they aren't investing in ongoing training for their engineers, that's a red flag. Some business owners won't invest in training and give this excuse: "What if I spend all this money in training my employees and then they leave us for another job?"

Our response is, "What if you DON'T train them and they stay?"

Q14: How do you lock down our employees' PCs and devices to ensure they're not compromising our network?

Like the above, the question may get a bit technical. The key is that they HAVE an answer, and don't hesitate to provide it. Some of things they should mention are:

- Do you use 2FA (two-factor authentication) and enforce this as a policy?

- Do you install and manage Advanced end-point protection?
- When someone has an intrusion or accesses harmful information, does your office know about it and if so do you have a written process to stop such problems?
- Are you able to isolate a users computer from the network at any moment a virus or intrusion is suspected?
- Do you provide reports on a regular bases for our management team to know who has access to company computers?

Q15: What cyberliability and errors and omissions insurance do you carry to protect me?

Here's something to ask about: if THEY cause a problem with your network that causes you to be down for hours or days, to lose data or get hacked, who's responsible? What if one of their technicians gets hurt at your office? Or damages your property while there?

In this litigious society we live in, you better make darn sure whomever you hire is adequately insured with both errors and omissions insurance, workers' compensation and cyberliability – and don't be shy about asking them to send you the policy to review!

If you get hit with ransomware due to their negligence, someone has to pay for your lost sales, the recovery costs and the interruption to your business operations. If they don't have insurance to cover YOUR losses of business interruption, they might not be able to pay and you'll have to end up suing them to cover your costs. If sensitive client data is compromised, who's responsible for paying the fines that you might incur and the lawsuits that could happen? No one is perfect, which is why you need them to carry adequate insurance.

True story: A few years ago a company that shall not be named was slapped with several multimillion-dollar lawsuits from customers for bad behavior by their technicians. In some cases, their techs where accessing, copying and distributing

personal information they gained access to on customers' PCs and laptops brought in for repairs. In other cases, 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.

Q16: Who audits YOUR company's cyber security protocols and when was the last time they conducted an audit?

Nobody should proofread their own work, and every professional IT consulting firm will have an independent third party reviewing and evaluating their company for airtight cyber security practices.

There are many companies that offer this service, so who they use can vary (there's a number of good ones out there). Bottom line, if they don't have a professional cyber security auditing firm doing this for them on at least a quarterly basis, or if they tell you they get their peers to audit them, DO NOT hire them. That shows they are not taking cyber security seriously.

For instance, even in my IT company we use an third party who specializes in IT security to test our company systems. We also use them to review and test our client systems. Yes, even though my company has fully certified security experts, we use Certified Third-Party contractor to oversee our work.

Q17: Do you have a SOC and do you run it in-house or outsource it? If outsourced, what company do you use?

A SOC (pronounced "sock"), or security operations center, is a centralized department within a company to monitor and deal with security issues pertaining to a company's network.

What's tricky here is that some IT firms have the resources and ability to run a good SOC in-house (this is the minority of outsourced IT firms out there). Others cannot and outsource it because they know their limitations (not entirely a bad thing).

But the key thing to look for is that they have one. Less experienced IT consultants may monitor your network hardware, such as servers and workstations, for uptime and patches, but they might not provide security monitoring. This is particularly important if you host sensitive data (financial information, medical records, credit cards, etc.) and fall under regulatory compliance for data protection.

Q18: Have you, or any of your clients, ever been hit with ransomware or a major breach?

This is a tough question that will put them on the spot for sure. If they have been hit with ransomware or a major breach, I would not classify them as a "bad" IT company if they said yes to this question. What I would want to know is how it happened and what they have done to ensure it doesn't happen again. I would like to know how they handled the situation, how it impacted their clients and what they did in response to the breach.

Sadly, it's almost a question of "when," not "if," you get breached. At the time of writing this book, there have been breaches of MSPs that have been caused at the vendor level, not due to the fault of the MSP.

However, they should be open, honest and straightforward with their answer. If they get angry, defensive or appear to be covering something up, those are definitely warning signs you don't want to ignore. Or they may put all the blame on the client and not take any responsibility, that too is a warning sign. It will show how they will treat you if ever there is a problem.

Backups And Disaster Recovery:

Q19: Can they provide a timeline of how long it will take to get your network back up and running in the event of a disaster?

There are two aspects to backing up your data that most business owners don't realize. The first is "fail over" and the other is "fail back."

For example, if you get a flat tire when driving, you would "fail over" by putting the spare tire on to get you home or to a service station where you can "fail back" to a new or repaired tire.

If you were to have a disaster that wiped out your data and network, be it a ransomware attack or natural disaster, you want to make sure you have a "fail over" solution in place so your employees could continue to work with as little interruption as possible. This fail over should be in the cloud and locked down separately to avoid ransomware from infecting the backups as well as the physical servers and workstations.

But at some point you need to "fail back" to your on-premise network, and that's a process that could take days or even weeks. If the backups aren't done correctly, you might not be able to get it back at all.

So, one of the key areas you want to discuss in detail with your next IT consultant or firm is how they handle both data backup AND disaster recovery. They should have a plan in place and be able to explain the process for the emergency "fail over" as well as the process for restoring your network and data with a timeline.

In this day and age, regardless of natural disaster, equipment failure or any other issue, your business should ALWAYS be able to be operational with its data within six to eight hours or less, and critical operations should be failed over immediately.

Q20: 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?

A great IT consultant will place eyes on your backup systems every single day to ensure that backups are actually occurring, and without failures.

However, in addition to this, your IT company should perform a monthly randomized "fire drill" test restore of some of your files 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.

If you don't feel comfortable asking your current IT company to test your backup OR if you have concerns and want to see proof yourself, just conduct this little test: Copy three unimportant files onto a thumb drive (so you don't lose them) and delete them from your server. Make sure one was newly created the same day, the other a week old and the last one a month old.

Then call your IT company and let them know you've lost three important documents and need them restored from backup as soon as possible. They should be able to do this easily and quickly. If not, you have a problem that needs to be addressed immediately!

Verifying your backups daily and actually testing them on a regular basis is a cornerstone of a successful overall IT strategy.

I decided a long time ago regarding the type of backup and disaster equipment and service I wanted for my clients. After having to deal with a curupted database a client had and went to restore one from an external backup service, I found out that the backup was not being done completely. It was never tested on a regular basis and thus when we went to restore it, the latest version was not going to work. It was very fortunate that we did have an older version that did work, but I know at that time this was not good enough.

Q21: If you were to experience a location disaster, pandemic shutdown or other disaster that prevented you from being in the office, how would they enable you and your employees to work from a remote location?

If 911 taught us anything, it showed us that even a backup plan can go wrong. Many had external backup devices that they would bring home each night and then back the next day to swap-out, but during the attack the quick exit from the building they did not have any of the backups and thus when the building collapsed all the information (much of it financial) was gone. Also, Covid taught us anything, it's that work-interrupting disasters CAN happen and DO happen when you least expect them. Fires, floods, hurricanes and tornados can wipe out an entire building or location. Covid forced everyone into lockdown, and it could happen again.

We could experience a terrorist attack, civil unrest or riots that can shut down entire cities and streets, making it physically impossible to get into a building. Who knows what could be coming down the pike. Hopefully NONE of this will happen, but sadly it does.

That's why you want to ask your prospective IT consultant how quickly they were able to get their clients working remote (and securely, I might add) when Covid shut everything down. Ask to talk to a few of their clients about how the process went.

Q22: Show me your process and documentation for onboarding me as a new client.

The reason for asking this question is to see if they HAVE SOMETHING in place. A plan, a procedure, a process. Don't take their word for it. Ask to SEE it.

You might not understand a single part of it, but that's not what's important here. What's important is that they can produce some type of process. Further, they should be able to explain how that process works.

One thing you will need to discuss in detail is how they are going to take over from the current IT company – particularly if they are hostile. It's disturbing to me how many IT companies or people will become bitter and resentful over being fired and will do things to screw up your security and create problems for the new company as a childish way of getting revenge. A good IT company will have a process in place for handling this (sadly, it's more common than you think).

Q23: Ask them who will be their IT consultant?

In many cases you may only get a client manager who is realy a salesperson and not an IT person who understands your network and computer systems. They may say they have engineers to assist the salesperson. You may want to meet that person as well, so you know who is working on your business network. Will you get the same person each time they have to come to your office, or will it be just any IT person available. Are they going to have to learn on your time and dime?

Other Things To Notice And Look For:

Are they good at answering your questions in terms you can understand and not in "geek-speak"?

Good IT companies won't confuse you with techno-mumbo-jumbo, and they certainly shouldn't make you feel stupid for asking questions. All great consultants have the "heart of a teacher" and will take time to answer your questions and explain everything in simple terms. As you interact with them in the evaluation process, watch for this.

Do they and their technicians arrive on time and dress professionally?

Do their technicians present themselves as true professionals when they are in your office? Do they dress professionally and show up on time?

If you'd be embarrassed if YOUR clients saw your IT consultant behind your desk, that should be a big red flag.

How you do anything is how you do everything, so if they cannot show up on time for appointments, are sloppy with paperwork, show up unprepared, forget your requests and seem disorganized in the meeting, how can you expect them to be 100% on point with your IT? You can't. Look for someone else.

Do they have experience in helping clients similar to you?

Do they understand how your business operates the line-of-business applications you depend on? Are they familiar with how you communicate, get paid, service your clients or patients and run your business?

Obviously, someone who works with other clients similar to yours should

The SuperSTAR IT Consultant You Want Vs. A SuperSCREWup You Don't Want

SuperSTAR	SuperSCREWup
Has proven qualifications and experience, is vendor-certified	Is just getting started, has less than a year in business, has no tangible qualifications
Offers managed IT services that include advanced cyber security protections (more than just a firewall)	Offers "break-fix" services and lacks the ability to offer advanced cyber security protections
Is fully insured (liability, cyberliability and workers' compensation)	Has no insurance or insufficient insurance coverage
Has several client references and online reviews	Has no references, testimonials or reviews (or very few)
Has multiple technicians and teams to support you	Has no backup team, works alone, no "Plan B"
Has a local, company-owned help desk and dedicated SOC	Is outsourcing their help desk to a third-party vendor, no SOC
Guarantees response times and has documented response systems in place (30 minutes or less)	Has no response system or guarantees, won't commit to anything
Consistently documents all discussions, deliverables, guarantees and project timelines in writing	Prefers verbal communication, never follows up with written agreements
Provides you detailed reporting and updates	Provides no reports or status updates
Provides network documentation	Doesn't offer network documentation, or charges more for it

The SuperSTAR IT Consultant You Want Vs. A SuperSCREWup You Don't Want

SuperSTAR	SuperSCREWup
Has an established office	Has no office, uses a P.O. box and a cell phone working from home
Provides all timelines, prices and service-level guarantees in writing	Provides vague project outlines, time and materials pricing; offers "window" timelines
Shows up on time, every time	Shows up late or not at all, makes excuses
Sends correct, detailed invoices	Invoices are incorrect, never on time and pile up to later hit you with a giant bill you didn't expect
Is easy to reach, returns calls promptly	Is hard to reach
Resolves problems quickly and documents what happened so problems don't reoccur	Is haphazard about resolving problems; same ones occur again and again
Is always professionally dressed, polite and respectful	Is sloppy, smells bad, has a disheveled appearance and is rude
Uses systematic follow-up to ensure your satisfaction	Uses no follow-up; no contact 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

Chapter 5:
Options For Getting The IT Support You Need

When you think about getting IT support for your business, there are a lot of options to choose from and companies providing IT support. But which one is the best for you? In this chapter, I'm going to lay out the options you have and the pros and cons of each.

Option #1: Don't do anything UNTIL something breaks or stops working.

This is really foolish, but we see it every day: businesses that don't pay attention to the care and maintenance of their computer 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 no different than ignoring the "change oil" light in your car until smoke starts pouring out from under the hood. Taking a reactive approach to IT support is a surefire path to getting hit with ransomware and losing data, as well as having ongoing IT issues that slow you and your staff down.

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 make sure you don't fall victim to a cyber-attack and lose your data. A short list of these tasks includes:

- Security monitoring
- Verification of backups
- Security patches and updates
- Disaster recovery planning
- Server and desktop optimization
- 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 (such as financial or medical organizations, any government agencies or any company that has regulatory compliance considerations) or other specialized needs, the list is even longer.

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 IT problems as they arise. Aside from your staff members, your network and the data on it are undoubtedly some of the most valuable assets your business possesses – client data, contracts, work product, conversation histories, e-mails and more.

As the old saying goes, an ounce of prevention is worth a pound of cure; this goes double for your computer network. Unfortunately, some business owners are too cheap and end up paying for it in other ways. Stupid.

Option #2: Outsource to a friend/brother/cousin or other "cheap" alternative who is "good with tech."

Trying to save a buck by hiring someone who will work for beer money is a false savings. They could end up doing more damage than good and never really

resolve the problem – and they most certainly won't be able to recover you from a ransomware attack or disaster situation.

Along this same line is designating 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 they can't solve.

The problem is, you are pulling these people away from the main job you hired them to do, and unless they have 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 do a great job. This inevitably results in a network that is poorly maintained and unstable, which may cause excessive downtime, overspending on IT support and expensive recovery costs.

Another variation of this is to get your neighbor's kid or a friend to provide IT support on a part-time basis.

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: Build your own internal IT team.

Sometimes it makes sense to have a full-time IT person to support your network, but there are limitations you need to be aware of.

First of all, no one IT person can know everything there is to know about IT support and cyber security. If your company is big enough and growing fast enough to support a full-time engineer, you probably need more than one guy. You need someone with help-desk expertise as well as a network engineer, a network administrator, a CIO (chief information officer) and a CISO (chief information security officer).

Therefore, you may still need to supplement their position with co-managed IT support using an IT firm that can fill in the gaps and provide services and expertise they don't have. This is not a bad plan; what IS a bad plan is hiring one person and expecting them to know it all and do it all.

Second, finding and hiring good people is difficult; finding and hiring skilled IT people is incredibly difficult due to the skill shortage for IT. And if you're not technical, it's going to be very difficult for you to interview candidates and sift and sort through all the duds out there to find someone with good skills and experience. Because you're not technical, you might not know the right questions to ask during the interview process or the skills they need to do the job.

More often than not, the hard and soft costs of building an internal IT department for general IT support just doesn't provide the best return on investment for the average small to mid-size business and typically doesn't make sense until you have closer to 150 employees. There certainly are times when it's right to bring on internal IT staff when you need specialized skills, a developer, etc., but not for day-to-day IT support and maintenance.

Option #4: Use the IT support offered by your ISP or other big-tech vendors.

A number of big-tech companies, like Best Buy, Staples, Local Internet/ Phone company offer IT business support – but buyer beware!

If you've ever tried to get technical support from your phone company or ISP, you know how frustrating it can be. Consider the last time you called your ISP for an Internet outage; how easy was the process? I'll bet you dreaded making the call and experienced a significant blood pressure spike as you waited on hold and dealt with unhelpful "customer service" people who ran you in circles. This is why we don't recommend you choose this option.

First, many vendors don't provide personalized support with a dedicated team who get to know you and your company. You're one among a thousand customers and you're treated that way.

True experience regarding a big Internet Services Provider offering Security protection within the service they have and telling a client they do not need anything more. A new client who had a contract with a Very Large ISP needed to make a change to the so called firewall (the ISP said the Modem was a firewall along with the security-edge protection), but when the client asked the support person how to change that so called powerful Security-Edge protection, they did not know how and in fact no one in support did. This was a problem, and it halted work for that client till we got involved and had the ISP remove the Security-Edge protection, oh and get this, the ISP was still going to charge them for the service.

It's not uncommon for the support staff to be located in another country, and they 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. Believe it or not, we've found tweeting or reaching out on social media often gets faster response than trying to reach an actual live human being who can help you.

Here's another problem with these types of support plans: they are very limited in scope and won't 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 ISP. 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. Maybe the cleaning crew disconnected a wire by accident. If your problem is even partially related to another software or piece of hardware on your system, they won't help you. As I'm sure you know, it is virtually impossible to get two different vendors to talk to each other to fix a problem, much less work together to implement a system that resolves network downtime for good. Finger-pointing is the name of the game and you're left on your own to figure things out.

If you have that kind of spare time to troubleshoot your own IT and deal with the useless customer service teams at these big companies, have at it.

Option #5: Outsource your support to a competent, local and independent IT consulting firm.

Yes, I'm biased when I say this is often the BEST option for small businesses, 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 40 years, so I have considerable experience working with – and talking to – thousands of other small-business IT consultants. I've seen the horror stories and heard the complaints business owners have with other technology service vendors. I've worked with the small business who nearly lost everything before they called us because of bad decisions they made themselves, and sometimes because of bad decisions made by incompetent technicians they've been working with. Based on that experience, I think the best option for a small business is an independent consulting firm that is locally owned and operated.

A small firm can provide personalized service. They can become an extension of your team and assist you in ensuring everyone is working at optimal levels.

The IT firm you choose should be large enough to provide backup 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 to hundreds of small to medium businesses in Vermont, and surrounding states, I have even had clients in Canada, Florida, Maine.

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. But I am confident in recommending that all small and mid-size businesses find and partner with an IT company they can trust and that will grow with them.

Chapter 6:
What Should You Expect To Pay For IT Services And Support?

One of the most commons questions we get from new, prospective clients calling our office is "What do you guys charge for your services?" They're trying to determine how our fees stack up against those of other IT firms.

Problem is, there are different approaches to charging for IT support, and looking at someone's hourly rate can't give you a true comparison of the end price or the true cost. If a company charges $99 per hour but puts a junior tech on the job, the tech might take three hours to do something that another company would charge $150 per hour for but complete in 30 minutes. Then, of course, there's the question of whether or not it's done *right*.

So, to better understand what you should be paying for IT support, I want to start by mapping out three predominant pricing models you'll encounter. They are as follows:

Time And Materials. In the industry, we call this "break-fix" services. Essentially, you pay an agreed-upon hourly rate for a technician to "fix" your problem when something "breaks." This is the most simple and straightforward way to charge for IT services, and most people like it for that reason. However, this doesn't work in your favor and can lead you to overpaying for services (more on this in a minute).

Managed IT Services. This is a model where the IT services company takes the role of your "IT department" for a fixed, agreed -upon monthly fee. For that fee, they install, support and maintain all the users, devices and PCs connected to your network on a routine basis. Hardware and software are all extra.

Many people like this arrangement because it allows them to budget for IT services and get the routine maintenance and IT support they need without having to hire a full IT department. This is a very common model, and the companies offering this are called MSPs, short for managed services providers. Often, these plans won't cover everything IT-related, so you have to be very careful about understanding what is and isn't included in that monthly fee. It's not uncommon for projects, adds and changes to your network to be billed as a project on top of the monthly fee for IT support.

TaaS. Some IT firms sell their services using a "technology as a service" model, which is very similar to the above managed services model but includes new hardware, software and support. This ensures you always have the most up-to-date hardware and software available without having one big out-of-pocket cost for a hardware refresh or software upgrade. This may not cover third-party software, so just like the above managed services model, you need to clarify what is and isn't included.

The upside of this is that you avoid the heavy cash outlay for hardware and software if you need it. The downside is that, over time, you'll pay FAR MORE for the same hardware and software, similar to leasing a car.

Of course, some IT firms offer all three options; some only offer one. So, let's look into which one is best for you and your situation.

Managed Services Vs. Break-Fix Hourly Support

You've probably heard the famous Benjamin Franklin quote "An ounce of prevention is worth a pound of cure." I couldn't agree more – and that's why it's my sincere belief that the managed IT approach is, by far, the most cost-effective, smartest option for any business.

The only time I would recommend a "time and materials" approach is when you already have a competent IT person or team proactively managing your IT and simply have a specific project to complete that your current in-house IT team doesn't have the time or expertise to implement (such as a network upgrade, migration, application development project, etc.).

Outside of that specific scenario, I do not think the break-fix approach is a good idea for general IT support for one very important, fundamental reason: you'll ultimately end up paying for a pound of "cure" for problems that could have easily been avoided with an "ounce" of prevention.

The fact of the matter is, computer networks absolutely need ongoing maintenance and monitoring to stay secure. Our ever-increasing dependency on IT systems and the data they hold – not to mention the type of data we're now saving digitally – has given rise to very smart and sophisticated cybercrime organizations that work around the clock to do one thing: compromise your networks for illegal activities and hold you ransom.

Of course, this doesn't even take into consideration other common "disasters," such as rogue employees, lost devices, hardware failures (the #1 reason for data loss), fire, natural disasters and a host of other issues that can interrupt or outright destroy your IT infrastructure and the data it holds. Then there's regulatory compliance for any business hosting sensitive information, such as credit cards, financial information, medical records and even e-mail addresses and phone numbers.

Preventing these problems and keeping your systems up and running (which is what managed IT services is all about) is a LOT less expensive and damaging to your organization than waiting until one of these things happens and then paying for emergency IT services to restore your systems (break-fix).

Why "Break-Fix" Works Entirely In The Consultant's Favor, Not Yours

Under a "break-fix" model, there is a fundamental conflict of interests between you and your IT firm. The IT services company has no incentive to stabilize your computer network or resolve problems quickly because they are getting paid by the hour; therefore, the risk of unforeseen circumstances, scope creep, learning-curve inefficiencies and outright incompetence are all shifted to YOU, the customer. Essentially, the more problems you have, the more they profit, which is precisely what you DON'T want.

Under this model, the IT consultant can take the liberty of assigning a junior (lower-paid) technician to work on your problem who may take two to three times as long to resolve an issue that a more senior (and more expensive) technician may have resolved in a fraction of the time. There is no incentive to properly manage the time of that technician or their efficiency, and there is every reason for them to prolong the project and find MORE problems than solutions. Of course, if they're ethical and want to keep you as a client, they should be doing everything possible to resolve your problems quickly and efficiently; however, that's akin to putting a German shepherd in charge of watching over the ham sandwiches. Not a good idea.

Second, it creates a management problem for you, the customer, who now has to keep track of the hours they've worked to make sure you aren't getting overbilled; and since you often have no way of really knowing if they've worked the hours they say they have, it creates a situation where you really, truly need to be able to trust they are being 100% ethical and honest AND tracking THEIR hours properly (not all do).

And finally, it makes budgeting for IT projects and expenses a nightmare since they may cost zero one month and thousands the next.

So, What IS A Fair Price?

Most IT services companies selling break-fix services charge between $100.00 and $120.00 per hour, with a one-hour minimum. In most cases, they will give you a discount of 5% to as much as 20% on their hourly rates if you purchase and pay for a block of hours in advance.

If they are quoting a project, the fees range widely based on the scope of work outlined and the specific skill set needed; a more sophisticated job (like implementing a security plan for a high-risk environment) will obviously cost more than setting up a standard PC for a new employee. If you are hiring an IT consulting firm for a project, I suggest you demand the following:

- A very detailed scope of work that specifies what "success" is. Make sure you detail what your expectations are in performance, workflow, costs, security, access, etc. The more detailed you can be, the better. Detailing your expectations up front will go a long way toward avoiding miscommunications and additional fees later on to give you what you REALLY wanted.
- A fixed budget and time frame for completion. Agreeing to this up front aligns both your agenda and the consultant's. Be very wary of loose estimates that allow the consulting firm to bill you for "unforeseen" circumstances. The bottom line is this: it is your IT consulting firm's responsibility to be able to accurately assess your situation and quote a project based on their experience. You should not have to pick up the tab for a consultant underestimating a job or for their inefficiencies. A true professional knows how to take into consideration those contingencies and bill accordingly.

MSP firms will quote you a MONTHLY fee based on the number of devices they need to maintain, back up and support. In Burlington, VT, I've seen fees range from $100 to $500 per server, $30.00 to $250.00 per desktop and approximately $5 to $20 per smartphone or mobile device – but buyer beware!

"Managed services" is a generic term used to describe IT support paid for on a monthly basis, and managed services plans are as unique as snowflakes, with no two being exactly the same. Therefore, to truly compare the price of one MSP to another, you need to look at the specific details of the plan and what's included and what's extra. Someone selling "managed services" for $40 a user can simply not be delivering true managed services since the tools to do the job properly cost more than that. That type of plan might not include security tools, backup, help desk, etc.

Further, one company charging $70 per user can't automatically be considered "cheaper" than someone offering managed services for $140 per user UNTIL you look into the details of what you're getting for the money. Don't be fooled by companies selling "all you can eat" support plans. In my experience, there are carve-outs they will bill you for, and if they don't have that, they're not very knowledgeable about the potential projects, needs and situations that could arise.

For example, if your office gets destroyed by a natural disaster, would they rebuild everything from the backups at no extra cost? What about a ransomware attack they have to recover you from – is that included? I've seen other IT shops claim "all you can eat" until something like this happens or a major project arises – then they claim that's not covered and will try to bill you for it (see the chapter on contracts later in this book).

Bottom line, price is only ONE consideration when comparing IT providers. A cheaper IT firm that delivers a substandard service isn't a bargain, especially if their incompetence costs you a ransomware attack or lost data. Further, the most expensive firm isn't a guarantee you'll get top-level service either.

As I've been reiterating throughout this book, choose the right provider based on the value they bring, the peace of mind they provide and the criteria I've outlined.

Chapter 7:
How To Choose An IT Company That Will Stand With You Against The Tsunami Of Cybercrime

When you fall victim to a cyber-attack through no fault of your own, will they call you stupid…or just irresponsible?

The above is a headline I've used in multiple places because it always grabs a CEO's attention. That's because it's true. Targets of all other crimes – burglary, rape, mugging, carjacking, theft – get sympathy from others. They are called "victims" and support comes flooding in, as it should.

But if your business is the target of a cybercrime attack where client or patient data is compromised, you will NOT get such sympathy. You will be instantly labeled "stupid" or "irresponsible." You may be investigated, and clients will question you about what you did to prevent this from happening – and if the answer is not adequate, you can be found liable, facing serious fines and lawsuits EVEN IF you trusted an outsourced IT support company to protect you. Claiming ignorance is not an acceptable defense, and this giant, expensive and reputation-destroying nightmare will land squarely on YOUR shoulders. But it doesn't end there…

According to your State laws (in my State of Vermont we are required), you may be required to tell your clients and/or patients that YOU exposed them to cybercriminals. Your competition will have a heyday with this. Clients will be

irate and could leave you in droves. Morale will tank and employees will blame you – and it's not uncommon for anonymous ex-employees to come out of the woodwork with stories of "They knew we were vulnerable, but did nothing about it." Your bank is not required to replace funds stolen due to cybercrime (go ask them), and unless you have a very specific type of insurance policy, any financial losses will be denied coverage.

Please do NOT underestimate the importance and likelihood of these threats. It is NOT safe to assume your IT company (or guy) is doing everything they should be to protect you right now; in fact, there is a high probability they are NOT, as we have discovered after doing dozens upon dozens of cyber security risk assessments in the last few years.

This is not a topic to be casual about. Should a breach occur, your reputation, your money, your company and your neck will be on the line, which is why you must get involved and make sure your company is prepared and adequately protected, not just ignore it.

Yes, It CAN Happen To You (And Probably Will At Some Point In The Future)

Far too many small-business owners stubbornly nobody wants access to our data." You are wrong, wrong, WRONG!

This is EXACTLY what cybercriminals are counting on you to believe so you'll let your guard down, putting ZERO protections in place, or grossly inadequate ones.

Right now, there are over 980 million malware programs out there and growing (source: AV-Test Institute), and 70% of the cyber-attacks occurring are aimed at small businesses (source: National Cybersecurity Alliance); you just don't hear about it because the news wants to report on BIG breaches OR it's kept quiet by the company for fear of attracting bad PR, lawsuits and data-breach fines – and out of sheer embarrassment.

In fact, the National Cybersecurity Alliance reports that one in five small businesses have been victims of cybercrime in the last year – and that number includes only the crimes that were reported. Most small businesses are too embarrassed or afraid to report breaches, so it's safe to assume that number is much, much higher.

Are you "too small" to be significantly damaged by a ransomware attack that locks all your files for several days or more?

Are you "too small" to deal with a hacker using your company's server as ground zero to infect all your clients, vendors, employees and contacts with malware?

Are you "too small" to worry about someone taking your payroll out of your bank account? According to Osterman Research, the AVERAGE ransomware demand is now $84,000 (source: MSSP Alert). It's also estimated that small business lost more than $100,000 per ransomware incident and over 25 hours of downtime. Of course, $100,000 isn't the end of the world, is it? But are you okay to shrug this off? To take the chance?

It's NOT Just Cybercriminals Who Are The Problem

Most business owners erroneously think cybercrime is limited to hackers based in China or Russia, but the evidence is overwhelming that disgruntled employees, both of your company and your vendors, can cause significant losses due to their knowledge of your organization and access to your data and systems. What damage can they do?

They leave with YOUR company's files, client data and confidential information stored on personal devices, as well as retaining access to cloud applications, such as social media sites and file-sharing sites (Dropbox or OneDrive, for example) that your IT department doesn't know about or forgets to change the password to.

In fact, according to an in-depth study conducted by Osterman Research, 69% of businesses experience data loss due to employee turnover and 87% of employees who leave take data with them. What do they do with that information? Sell it to competitors, BECOME a competitor or retain it to use at their next job.

They can steal money, inventory, trade secrets and client lists. There are dozens of sneaky ways employees steal, and it's happening a LOT more than businesses care to admit. According to the website StatisticBrain, 75% of all employees have stolen from their employers at some point. From inventory theft to check and credit card fraud, your hard-earned money can easily be stolen over time in small amounts that you simply never catch or discover.

Here's one of the most COMMON ways they steal: they waste HOURS of time on your dime to do personal errands, shop, play games, check social media feeds, gamble, read the news and a LONG list of non-work-related activities. Of course, YOU are paying them for a 40-hour week, but you might only be getting half of that. Then they complain about being "overwhelmed" and "overworked." They tell you, "You need to hire more people!" so you do. All of this is a giant suck on profits if you allow it.

Further, if your IT company is not monitoring what employees do and limiting what sites they can visit, they could do things that put you in legal jeopardy, like downloading illegal music and video files, visiting adult content websites, gaming and gambling – all of these sites fall under HIGH RISK for viruses and phishing scams.

Another way an employee can burn you on the way out: they DELETE everything. They get fired or quit – but before they leave, they permanently delete ALL their e-mails and any critical files they can get their hands on. If you don't have that data backed up, you lose it ALL. Even if you sue them and win, the legal costs, time wasted on the lawsuit and on recovering the data, not to mention the aggravation and distraction of dealing with it all, are all greater costs than what you might get awarded if you win the lawsuit, or what you might collect in damages.

How To Work With Your IT Company To Get The Best Protection

Protecting your organization from cybercrime and ransomware is a partnership between you and your IT company. Yes, they need to put in place systems and protocols to protect you – but you also need to do your part in ensuring that their efforts aren't compromised or circumvented by your employees, or that you're tying their hands and making it impossible for them to protect you.

Let Them Do Their Job! I know I sound like a broken record, but allow your IT company to monitor and maintain your network 24/7/365 and install critical cyber security protections that will keep you from falling victim. If they tell you it's important to add a protection, upgrade a device or purchase a better backup solution, listen to them! You cannot expect them to protect you if you're constantly telling them, "I don't need all of that" or "I don't want to spend the money on that!"

This is why you need to find an IT company you can trust. If they are recommending it, you can trust them that it's actually something that's necessary and not a frivolous recommendation designed to pad their pockets.

Advanced Endpoint Protection. Antivirus is nearly useless against the threats happening today, so you need a more sophisticated approach to protecting your network. If all your IT company offers is antivirus, it's time you find another IT company. A good IT consultant will guide you through more advanced protections today that will greatly reduce your chances of a cyber-attack happening.

Employee Cyber Security Awareness Training. Employees are the single biggest threat to your company's security. All it takes is one employee using a weak password or unsuspectingly clicking on a shared Google Doc link in an e-mail, and they could unleash a malware program that will take down your entire system within minutes. That's why we recommend providing some security training on

an ongoing basis to keep your employees hypervigilant against phishing attacks, suspicious e-mails and links, and downloading files that can circumvent security protocols and infect your network.

Implementation Of An AUP (Acceptable Use Policy). An AUP is a document that details to your employees how they are permitted to use company e-mail, Internet, data and devices to protect you from potential lawsuits, data breaches and confidential information being shared or stolen.

For example, employees might think it's perfectly acceptable to visit a gambling website during lunch, which infects your network with nefarious programs designed to steal data and install ransomware. They might think it's okay to use company Internet to connect to porn sites on their phone, creating the potential for a sexual harassment lawsuit, not to mention a cyber security problem. They might event think it's acceptable to upload sensitive data (client files, credit cards, etc.) to unsecured websites.

Your IT company can not only help you create this document and the rules (while working with your HR department and employment attorney) but can also enforce rules such as blocking certain types of websites from your network or preventing employees from accessing unapproved web applications for data sharing and downloading unapproved and unsecured applications (like screen savers, "enhanced" web browsers, pirated music files, etc.).

2FA And Strong Passwords. 2FA, or "two-factor authentication," is a process where an employee must use a password and some other type of authentication to prove they are who they say they are. For example, you might need to authorize access via a cell phone in addition to logging in with a password. Using this for critical applications greatly increases the security of those applications and devices.

Another key to strong security is long, complex and unique passwords. Talk to your IT company about how they can enforce good password policies for your employees so they don't get lazy and use "letmein" or "password" as their password.

Of course, these are just a few things to look for. Everyone's situation is slightly different and you need the expertise of a good IT consultant to assess your situation and make recommendations that are right for you.

Chapter 8:
The Devil's In The Details: How To Read An IT Services Contract

Now that you've gone through the work of finding the perfect IT consultant, 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 consultant, ask to meet so that you can both 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 consultant to bring a copy of the original proposal or quote, as well as a list of deliverables, deadlines, guarantees and other policies and procedures.

Here are a few of the things to make sure you review before signing.

Warranties And Guarantees

One of the main things you want to clarify in your contract is exactly what your consultant does and does not guarantee. Make sure you are as specific as possible. For example, if a computer you purchase through your consultant has a hard-drive failure, will they be responsible for getting it replaced with the manufacturer or will you? If you experience a problem with the network that your consultant recently upgraded or installed, is support included or is it charged at an extra rate? Also, if you are unhappy with the work, what happens? Will the job be redone at no extra charge? Will you be refunded part or all of your money?

Payment Terms

If you are enrolling in a managed services plan, most payments will be done a month in advance for the work being delivered. That contract should be pretty straightforward.

However, if you are hiring them for a specific project, most consultants will require some type of down payment before getting started, and payment for any hardware or software purchases up front. However, you should never pay a consultant in full before a project is started for ALL services, 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 as much of the services payment as possible until full completion of the project. In some cases, that may be as much as 30% to 50%. Basically, you want to keep the final payment as large as possible 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 dates, amounts and specifically what work and conditions of satisfaction have to be met before payment is made. Don't be alarmed if your consultant includes a condition that all work will cease for nonpayment. This is standard and not unreasonable.

Remember to review with your consultant each step before releasing payments. Example of this was a client of mine that did not go through my services when contracting a software vender. They gave the client 50% up front and they never outlined any of the consultants target and functions that had to be working before payment. In the end they released all funds but never got a fully working program. The consultant said they met what was outlined in their contract, but the client did not understand what that target was.

Project Timeline And Completion Date

If your project is time-sensitive, you'll want to include not only a definite completion date, but also breach-of-contract terms that give you some type of compensation for every day or week over the deadline. 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 eleventh hour that your project is way overdue.

Important: Some projects will require your involvement in testing and approving applications and processes designed by your consultant. 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 that clients request to a project after the contract has been signed. In some cases, these "tiny" changes result in more work for the consultant and delays in the project's timeline.

For example, let's suppose you decide it's time to upgrade your network. Your consultant provides you with a game plan and a quote for what it will take to

perform the upgrade. 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 the hourly rate or amount for any changes is not unreasonable and is clearly defined in the contract you sign. In most cases, the consultant 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 consultant is a professional, they will require 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
- The new completion date for your project (if applicable)
- If they are using a Ticket system to keep track of their time, see if they will put that request in a new ticket and not part of an existing one. This helps you check and make sure of the time they quoted is accurate.

This document should be signed by both you and your consultant.

Hardware, Software And Materials

Many IT consultants will gladly research and quote the cost of various hardware and software for the completion of a project. Some will even offer to custom-build your server and workstations instead of purchasing them from a hardware distributor. In most cases, these non-branded computers are every bit as reliable as branded machines offered by Dell, HP or Lenovo. Either way, you want to keep in mind that your consultant is probably not making a lot of money on selling hardware and software and, in many cases, will only resell it to you as a convenience (one-stop shopping).

That's why you want to detail in your contract who is responsible for the warranty on the equipment. If something goes wrong, do you want your consultant to handle it or will you? Most consultants 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 a consultant work on your network is the downtime it costs you.

In some situations, it may be necessary for you and all your employees to log off the network so your consultant 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 consultant how much downtime the repair or project will require and when the

work will be done (evenings and weekends or during business hours). 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 consultants will gladly accommodate you if you ask in advance.

Getting Out Of The Contract

While this book is dedicated to helping you find a great consultant whom you will never want to fire, there still is a chance you could end up hiring the wrong one. If that happens, you want to make sure your contract is written to protect your rights and keep you from being taken advantage of. Again, this section should not be considered legal advice and should not take the place of a qualified attorney reviewing your contract. However, for the sake of completeness, we will touch on what you need to protect yourself in the event that your consultant doesn't fulfill promises.

For starters, make sure your contract has a clear cancellation policy. If you discover that you hired the wrong consultant and want out of your contract, you'll want a written clause that details not only how to cancel the contract, but also what you will owe. Determining whether you are entitled to a refund, or are required to pay for work completed, will often have to be negotiated.

Quick Tip: If you decide you need to cancel a contract, make sure you send your cancellation notice by certified mail, return receipt requested. This will give you proof that your consultant has received your cancellation notice.

The biggest "secret" to securing a win-win contract is to make sure there are no loopholes. Include everything you can think of in writing, no matter how small or insignificant it may seem at the moment.

And finally, you should always have a qualified legal consultant review your agreement, especially if it involves a lengthy and expensive project. The little bit of money you will invest in a good attorney will go a long way to ensuring a happier, low-hassle project!

Chapter 9:
What Is Co-Managed IT And When Does It Make Sense

Co-managed IT is simply an arrangement when an outsourced IT company supplements your in-house IT person or department with specific skills, tools and solutions.

When Should You Hire Or Outsource?

While outsourcing is common in many areas of business, such as HR, finance and procurement, the most mature and commonly outsourced function for businesses of all sizes is IT (information technology).

That's because it is almost always cheaper, easier and more advantageous to outsource at least some aspects of IT – including the support and management of your IT infrastructure, data backup and cyber security protections – than the cost and burden of building a robust internal IT department that can handle everything. However, the big question is what should you outsource and what should you keep in-house? In general, it's best to OUTSOURCE in the following scenarios:

- **When the job requires a highly specialized skill that is better handled by a team of experts.**

  For example, cyber security is one of the most commonly outsourced functions of IT and is growing. That's because protecting an organization against cybercrime is a business-critical function that cannot be pushed on to an individual IT person or team that lacks the deep knowledge, tools and

expertise required. Another example would be a critical migration project of on-premise networks to the cloud.

- **To save the time and cost of hiring.**

  Whenever you can find a vendor who can take on the tasks you're looking to hire for, they not only save you an enormous amount of time in regard to finding, interviewing, hiring and training new employees, but also save you money in HR, payroll and insurance costs. Specific to IT, you will also save money by not having to purchase the IT management tools, programs and applications they need to do their job properly.

- **When you need a flexible workforce.**

  If you have a seasonal business, or if you want the ability to scale up or down quickly, outsourcing is always the faster, less expensive option.

- **You simply don't want the added difficulty of hiring and managing an IT department.**

  For starters, the talent pool out there is brutal; simply finding a good IT person of any caliber is difficult. Then you have to take into consideration a "Plan B" if they leave or are suddenly unable to work. If you don't have someone who knows your systems as a backup, you can go through a VERY painful period of trying to hobble along until you replace them. This is why many of our larger clients who HAVE internal IT choose our CoMITs, which is short for co-managed IT services (more on this later).

From our experience, companies with fewer than 75 employees are almost always better off outsourcing 100% of the management of their IT (it's important to note that we're talking about the generic IT management).

At the 75-employee mark, it may make sense to have a strategic IT person on staff, based on the unique needs of your organization, but usually that person is managing a specific application or business function and still needs the help of an external IT company to assist in any number of things, particularly cyber security.

What Your IT Department Should Consist Of

Most companies don't fully understand all the skill sets required in a properly staffed, competent IT department. Once they do, they quickly see why:

- One IT person is not sufficient for most companies (particularly due to the complexity and deep expertise required for cyber security).
- Outsourcing is a less expensive option that would also give them FAR superior services and cyber security protection.

Below is a high-level overview of the various skill sets and functions you'll need for a competent IT department, even in a small 30-person company, and if you happen to be an organization that falls under strict data compliance guidelines, the number of employees is irrelevant – you MUST keep your patients' and clients' data safe even if you're a "one-man-band."

Title	Purpose	Employees	*Salary
Help Desk Technician (Levels 1-3)	Responsible for being the first line of defense to troubleshoot end-users' problems, questions and needs. Needs to be highly responsive.	1 per 70 employees	$35,000 - $50,000
Network Administrator	Responsible for maintaining your company's computer network (designed by the Network Engineer), ensuring it's up-to-date, secure and operating as intended.	1 per 200 employees	$55,000 - $90,000
Network/Systems Engineer	Responsible for the strategic planning and implementation of the communication networks in your company.	1 per 200 employees	$63,000 - $100,000
IT Manager	Responsible for managing the help desk, network administrator and systems engineer.	1 per 500 employees	$90,000 - $150,000
CIO (Chief Information Officer), CTO	Most senior technology executive inside an organization. Responsible for setting and leading the IT strategy for the entire company to ensure IT facilitates the goals of the organization.	1	$100,000 -$150,000
CISO (Chief Information Security Officer)	Responsible for being head of IT security, creating, implementing and managing a company's IT security policies to prevent a breach.	1	$185,000 - $250,000
Total			$438,000 - $640,000

It's important to keep in mind that most will not need the above individuals' expertise 24/7/365 (like the CISO), but you WILL need that expertise at some level. Further, your IT department will need the following applications and tools to do their job properly:

- Help-desk ticket management system
- Remote monitoring tools
- IT documentation
- IT hardware test equipment
- Utility software such as predefined scripts for software management.
- Up-to-date computer systems and monitors. Do not let them use old or outdated equipment, this will slow them down.
- A space to maintain and pre-deploy computer equipment.

How Co-Managed Works

Many of the clients we work with have one or more internal IT people but are growing and finding they need additional support. Instead of hiring for EVERY role, they are opting for a new form of outsourced IT services we call Co-Managed IT, or CoMITs for short.

Co-managed IT gives companies the helping hands, specialized expertise and IT management and automation tools they need WITHOUT the cost and difficulty of finding, managing and retaining a large IT staff OR investing in expensive software tools.

Here's What Co-Managed IT Is NOT

- It's NOT about taking over your IT leader's job or replacing your IT department if you have one or more people who are productive, strategic members of your team.

- It's NOT a one-off project-based relationship where an IT company would limit their support to an "event" and then leave your team behind to try and support it (or give you the option to pay them big bucks afterwards to keep it working).
- It's NOT just monitoring your network for alarms and problems, which still leaves your IT department to scramble and fix them.

It IS a flexible partnership where we customize a set of ongoing services and software tools specific to the needs of your IT person or department that fills in the gaps, supports their specific needs and gives you far superior IT support and services at a much lower cost.

There are several benefits to co-managed. The first (and most obvious) is that we make your IT person or team BETTER. By filling in the gaps and assisting them, giving them best-in-class tools and training, and freeing them to be more proactive and strategic, we make them FAR more productive for you. As an added bonus, THEY won't get burned out, frustrated and leave.

Second, you don't have to add to your head count. Let's face it: overhead walks on two legs. Plus, finding, hiring and retaining TOP talent is brutally difficult. With co-managed IT, you don't have the cost, overhead or risk of a big IT team and department. We don't take vacations or sick leave. You won't lose us to maternity leave or an illness, or because we have to relocate with our spouse or we've found a better job.

Third, your IT team gets instant access to the same powerful IT automation and management tools we use to make them more efficient. These tools will enable them to prioritize and resolve your employees' problems faster, improve communication and make your IT department FAR more effective and efficient. These are software tools your company could not reasonably afford on its own, but they are included with our co-managed IT program.

Also not to be overlooked is that you get a "Plan B" backup team (without hiring them), in the unexpected event your IT leader is unable to perform their job OR if a disaster were to strike that requires a team and "all hands on deck." In those scenarios, we could instantly provide additional support people and resources to prevent the wheels from falling off. Which leads me to another critical benefit of co-managed IT…

You get a TEAM of smart, experienced IT pros working on your behalf. No one IT person can know it all, and giving your IT leader access to a deep bench of expertise to figure out the best solution to a problem, to get advice on a situation or error they've never encountered before and to help decide what technologies are most appropriate for you (without having to do the work of investigating them ALL), is a huge time and money saver for your company.

All of this also will give you greater peace of mind about not falling victim to a major cyber-attack, outage or data-erasing event. In our company, we assist IT leaders in implementing next-gen cyber security protections to prevent or significantly mitigate the damages of a ransomware attack or security breach. We provide end-user awareness training and help your IT leader initiate controls to prevent employees from doing things that would compromise the security and integrity of your network and data – and critical maintenance that often gets neglected or delayed actually gets done instead of piling up.

Scenarios Where Co-Managed IT Is Absolutely The Best Option

Scenario 1: Your in-house IT staff is better served working on high-level strategic projects and initiatives but needs support in getting day-to-day tasks completed, such as troubleshooting various problems that arise, providing help-desk resources to your employees, software upgrades, data backup and maintenance, etc.

Scenario 2: Your in-house IT person is excellent at help-desk and end-user support but doesn't have the expertise in advanced cyber security protection, server maintenance, cloud technologies, compliance regulations, etc. As in Scenario 1, we let them handle what they do best and fill in the areas where they need assistance.

Scenario 3: A company is in rapid expansion and needs to scale up IT staff and resources quickly. This is another situation where our flexible support services can be brought in to get you through this phase as you work to build your internal IT department.

Scenario 4: You have an excellent IT team, but they could be far more efficient if they had the professional-grade software tools we use to be more organized and efficient, along with our help desk. We can give them the tools, configure them for your organization and train them on how to use them. These tools will show you, the CEO, the workload they are processing and how efficient they are (we call it utilization).

Scenario 5: You have a robust in-house IT department but need on-site support and help for a remote location or branch office.

Who Co-Managed IT Is NOT For

Although there are a LOT of benefits to co-managed IT, this is certainly not a good fit for everyone. Here's a short list of people and situations this won't work for.

- **Companies where the IT leader is highly territorial and sees ANY outside help as an adversary instead of an ally.**

  Candidly, replacing the IT person or department IS the goal of some outsourced firms. They will attempt to get the internal IT person or team fired so the client can be dependent on them; therefore, this is not entirely an unfounded fear. But as I stated previously, our goal is not to have you fire your IT lead or your entire IT staff – our goal is to come in and be a resource in whatever way possible. Unfortunately, some IT managers just cannot get

beyond this concern and will dig their heels in and/or use passive-aggressive tactics to undermine the entire relationship and project. That's why co-managed IT only works when there is mutual trust and respect on both sides and a productive collaboration effort is made.

So, if you are a CEO who is bringing in an outside company, you need to keep this in mind. Your IT person might not want to "play nice" with someone they see as a threat, even if you know they need the help and you want to have a "Plan B" in place. We've seen CEOs insist, "Not MY guy… he wouldn't do that," only to have them be openly aggressive toward us, refusing to follow our recommendations, hiding information, dragging their feet and going back to the CEO with "bad news" about how the project is going. This is a tough path to navigate for you as the CEO and requires you to at least be aware of this if you make the decision to outsource some or all of your IT in a co-managed relationship.

- **IT leaders who don't have an open mind to a new way of doing things.**

  This is closely tied to the above problem.

  Our first and foremost goal is to support YOU and your IT leader's preferences, and we certainly will be flexible – we HAVE to in order to make this work.

  However, a big value we bring to the table is our 40 years of expertise in supporting and securing computer networks. Therefore, the clients we get the best results for are those that keep an open mind to looking at implementing our tools, methodologies and systems, and adopting some of our best practices. As I said before, this only works if it's a collaborative relationship. But we cannot – will not – take on a client that is doing things we feel compromise the integrity and security of a network, even if that's "how we've always done things" or because "that's what we like."

- **Organizations where the leadership is unwilling to invest in IT.**

  As a CEO myself, I completely understand the need to watch costs. However, starving an IT department of much-needed resources and support is foolish and risky. Further, some CEOs look at what they are paying us and think,

"We could hire a full-time person for that money!" But they forget that with us they are getting more than a single person – they are getting an entire team, a backup plan, tools and software, monitoring and specialized skills.

We can only help those companies that are willing to invest sufficiently in IT – not elaborately or indulgently. In fact, we can demonstrate how a co-managed IT option is a far cheaper solution than building the same team on your own.

Chapter 10:
Technical Terms Explained In Plain English

Backup and Disaster Recovery (BDR) Appliance:
A "BDR" is a device used to back up your servers and files that drastically reduces recovery time (fail over) should the actual server have a problem.

Unlike other backup technology, such as File and Folder Backup, or backing up to a USB drive, should your physical server fail, the BDR appliance can actually step in and assume the role of your server so that your employees can continue to work.

It also reduces recovery time from days down to two or three hours at most. It works because instead of backing up individual files, it takes a "snapshot" or picture of the entire server, including all of its files, on a regular basis, so it's sometimes called an "image-based backup."

Typically, a BDR will back up each server once an hour, so you should never lose more than an hour or two of work and data. It will also automatically store the data offsite in a data center so that if you have a physical disaster, such as a fire, hurricane, flood, etc., the data center can typically "turn your server back on" from the last backup and allow you to work from it.

Cable/Cable Modem:
A cable modem is a device provided by a cable television company that connects to your firewall to provide high-speed Internet to your firewall.

Cable Internet service is typically one of the fastest connections available to business, although it usually isn't as reliable or as fast as fiber. Cable Internet providers include companies like Comcast, TimeWarner and MediaCom.

Cloud Computing:
This is a general term to describe "Internet-based" computing, where shared resources, software and information are provided to computers and other devices on demand via the web. Facebook, Google search, websites and similar services are cloud services.

Cloud computing provides a means for you to have a server and network for your business that isn't physically inside your building, with all the same functionality and features.

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

Common content that businesses want to filter include pornography, gambling, workplace violence and hate-speech websites. Online shopping and social media are also popular types of content to block.

CPU:
C*entral* ***P****rocessing* ***U****nit*, the brains of a computer. Intel is the standard in business computer CPU choices. Some powerful computers, such as servers and those PCs used for drafting and 3D, have multiple processors.

DHCP:

***D**ynamic **H**ost **C**onfiguration **P**rotocol* relates to how computers and devices on your network receive the address used to talk to each other. Much like you have a street address at your office, your computer also has a street address on the network, as do all other devices. This is how your computer knows where to print your document to. Computer addresses, called IP addresses, can be assigned by your IT partner or can be obtained automatically. When a computer's address is obtained automatically, it's called DHCP. Your computer's network IP address was assigned by DHCP.

DNS:

***D**omain **N**ame **S**ystem (or **S**erver),* 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. In other words, if your computer wants to go to www.google.com, DNS tells it that it needs to go to the address 74.121.78.241.

Domain:

A technology used in Microsoft Windows Server operating systems. In layman's terms, it's what lets a server be a server. Your business's Windows Domain controls usernames and passwords, as well as password change requirements, and provides security for folders on the server so users can only see what their username gives them permission to see.

Domain Name:

Your Internet URL that typically will display your website when entered in a web browser and provides e-mail services @yourbusiness.com.

DSL:

***D**igital **S**ubscriber **L**ine*, a high-speed Internet service delivered over a telephone line. DSL connections are typically slower than fiber and cable connections. In addition, because it uses the copper phone network, it's not as reliable under most circumstances. If you have DSL and aren't using VoIP, even simple changes like plugging in an answering machine can cause problems, since DSL is using the same phone lines that the answering machine is connected to. It's our last recommendation only when fiber and cable aren't an option.

Exchange or Hosted Exchange:

A Microsoft software product typically used in businesses for e-mail functionality. Preferred over POP e-mail. In addition to sending and receiving e-mail, Exchange also allows you to share calendars and tasks with other staff in Microsoft Outlook. It also enables you to see your entire mailbox – including all subfolders underneath your in-box – on mobile devices like phones and tablets. If you move a message to a folder on your phone, it's in the same folder in Outlook on your computer and on your tablet. Another key differentiator and reason it's preferred for business e-mail needs is because it keeps your e-mail box on a server, whereas POP e-mail keeps messages on your computer. Exchange therefore allows you to quickly get another computer setup to receive e-mail, including having copies of all messages in all folders, as well as your address book on the new PC.

E-Mail Archival:

Archival, when speaking of e-mail, is a service that catalogues and securely keeps a copy of every single e-mail sent or received by anyone at your company, even if they permanently delete the message from their mailbox. Made more famous by the Hillary Clinton lost e-mail scandal, e-mail archival is something more industries and businesses are requiring their partners to utilize. Typically priced per user per month.

File and Folder Backup:

A type of backup where all the files and folders on a computer or server are copied, or backed up, to another location on a regular basis. Typically, this type of backup will either save a copy of all files onto a USB drive or an offsite backup

provider on a regular schedule. While this is a great choice for certain situations, a BDR image-based backup is preferred and will make the recovery process go much faster than a file and folder backup.

Firewall:
A firewall is a network security system (device or software application) that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted network (like your business) and an untrusted network, such as the Internet.

Fractional T-1 or MPLS:
In certain rural areas, in my State of Vermont broadband Internet such as fiber, cable, or DSL is not available or not sufficient. An MPLS (also called a T3, T1 or fractional T1, based on the Internet speed provided) connection is typically acquired from the phone carrier servicing the address where service is needed. While MPLS connections are costly, one notable difference between them and more traditional broadband connections is that the speed you pay for is guaranteed. Cable and DSL providers typically will only provide you a "best effort" to provide the speed they offer you. One local carrier considers it normal if your Internet download speed is 65% or more of the speed you pay for.

Hosted Applications:
This is a process of storing a software application in an offsite, usually third party, data center (cloud). Vendors are moving applications to this model and offering the service for a small recurring monthly fee, often based on number of users, instead of a more substantial onetime purchase. Microsoft's Office 365 is the most common example of a hosted application. Microsoft Exchange is a component of Office 365 that handles business e-mail.

IP Address:
See DHCP. An identifier for a computer or device on a network. Equivalent to a street address for a physical building. The format for an IP address is a 32-

bit numeric address separated by periods (example: 207.46.20.60). One notable thing that's important to understand is that there are both public and private IP addresses. Private IP addresses are assigned to devices inside your network. Public IP addresses are assigned to devices connected to the Internet (such as your firewall). Your internal computers, with private IPs, all originate from one public IP address assigned to the firewall.

A modern-day problem facing engineers is that as more devices are using Internet connectivity, there is a lack of available public IP addresses. Deep in nerd kingdom, IP addresses are based off a mathematic equation and there are a limited number of addresses available. The world is going to migrate to a newer form of IP addressing (essentially, a different mathematic equation) in the next several years to compensate for this problem.

IP Camera:
Typically a security or surveillance closed-circuit television camera that connects via network cable to your network to record video to a network video recorder (NVR).

Network Switch:
A network switch (or just "switch") is a device that connects the wired devices in an office together. Typically, each wall jack that a computer would plug into runs through the wall via Cat5e or Cat6 cable to a patch panel. From the patch panel, a patch cable connects that wire to the network switch. The network switch is directly responsible for the speed of the network – meaning a new switch will copy a very large picture from the server to your desktop faster than an old switch would. Almost all new switches are gigabit speed, which has been the standard for the past few years.

Switches are sold based on the number of ports – in other words, the number of wall jacks or number of devices that there are in a building. Switch configurations are typically 8 port, 16 port, 24 port or 48 port. In the event you need more than 48 connections, multiple network switches may be daisy-chained together.

Network Video Recorder (NVR):
A device that connects to your network typically to record and store video footage from IP surveillance cameras. The NVR is the device that your cameras record to and provides the means to remotely view those cameras via app or website. Also known as a DVR. An NVR may be a Windows-based PC but is often a standalone device.

Office 365:
An example of a hosted application, Microsoft offers their Office suite of products (Word, Excel, PowerPoint, Access, Outlook, Publisher, OneNote) as well as Microsoft Exchange e-mail services for a small monthly fee. Subscribers never have to purchase Office, as they are always allowed to have five copies of the latest (or any previous) version installed among their devices. For most businesses, an Office 365 subscription is $12 to $35 per month per user, and every staff member is legally required to have their own subscription. Prices for the subscription including Microsoft Access are slightly more expensive. Microsoft Visio and Project are also available via Office 365.

Patch Panel:
A telecommunications device typically in a server or utility closet that network jacks through a building will run and terminate into. Typically, each port is numbered. To facilitate easy cable management troubleshooting, it's common to label wall jacks with a number that corresponds to the port that wire connects to on the patch panel. Taking that a step further, it may also correspond to the network switch port. For example, a jack in an office number "3" will run to port 3 of the patch panel. A short patch cable will then connect port 3 of the patch panel to port 3 of the network switch.

POP3:
P*ost* ***O****ffice* ***P****rotocol 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. This is the type of e-mail you typically receive as part of

your Internet service and is typically not desirable for business. In the modern office environment, Microsoft Exchange (often through Office 365) or Google Apps is a more desirable e-mail solution. Among other reasons, if your e-mail service is POP-based, you are only able to see new e-mail messages on mobile devices like phones and tablets – you are not able to see your entire folder structure underneath your in-box. POP e-mail is the most affordable type of e-mail service offered and is often a good choice for home- or family-based e-mail addresses, just not businesses. For example, we provide POP e-mail services to the Smith family at thesmithfamily.org. They each have an @thesmithfamily.org POP e-mail box.

Power over Ethernet (PoE):
Power over Ethernet is a technology that allows an engineer to provide low-voltage power over the same network cable used for data transmission and reception to devices like wireless access points, VoIP telephones or IP cameras. For example, it's likely there will not be power at the locations where you wish to place surveillance cameras or wireless access points. Rather than have the expense and cost of having an electrician run wire and install power outlets at those locations, it's much easier to run a single network cable to the device. The device then uses that network cable for both data and power. A Power over Ethernet injector is the device that the other end of the cable connects to before it enters the network switch. This PoE injector typically provides between 4 and 24 volts of power to the device. Some network switches include the ability to provide PoE to some switch ports.

Protocol:
An agreed format for transmitting data between two devices. Think of protocol as you would language (English, Chinese, Spanish). Just as everyone in a meeting must speak English, all devices on a network must use the same protocol. TCP/IP is the standard for network protocol.

Remote Monitoring and Management (RMM):
A generic term for the software that IT consulting firms use to remotely and proactively monitor and maintain your network. RMM software is used for technicians to remotely access your computer, but that is only 5% of its

functionality. Properly configured RMM software will allow your consultant to perform a number of maintenance and problem resolution tasks without interrupting the user of the computer. When this is happening, the user often doesn't even know that work is being done.

RMM software is what allows us at Technology Consultants, Inc to be alerted to a possible impending problem and resolve that problem before it happens.

Server:
A computer or computers used on a network to provide security, centralized storage and shared folders, printers and applications. A server, while similar to a desktop computer, runs a server operating system. The difference between servers and workstations is that servers typically are more powerful and have redundancies built in so they have maximum availability. For example, servers will often save files to two or more drives in case one fails, and will have dual power supplies in case one power supply dies. Servers are typically either of a tower form factor or a rack mountable form factor. Tower servers resemble a computer tower, and rack-mounted servers mount in a telecommunications rack. This is desirable to save space and provide an added level of physical security, as racks will typically have doors that can be locked.

People sometimes have a misconception about servers as mysterious expensive boxes that sit in the closet. While this is true, to a degree, server technologies have changed in recent years and there are servers that are economical for every business size – from three users to upwards of 3 million users. A server for a small organization is likely more affordable than you'd imagine.

Spam/Spam Filtering:
Junk or unsolicited e-mail is known as spam. Once your e-mail address begins receiving junk mail, it's very hard to stop without changing your e-mail address. Spam filtering is a service that examines all e-mail before it is delivered to attempt to judge whether the message is legitimate or junk. If it's believed to be junk, it isn't delivered; instead, it's kept in a quarantine or separate folder from your in-

box. Many e-mail services, such as Google Apps/Gmail and Office 365 Hosted Exchange, provide basic spam filtering that works for most people. However, if you continue to receive junk mail that isn't being caught, a spam filter is required to provide more exhaustive junk mail filtering.

HINT: Don't use your primary work e-mail when you create accounts on websites or have to give your e-mail on a form. Instead, sign up for a free @gmail.com or @hotmail.com address and use that address when your address is requested by someone you aren't personally familiar with, like a colleague.

TCP/IP:
***T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol,* the basic language or protocol that governs traffic on the global Internet, as well as on most private networks.

URL:
***U**niform **R**esource **L**ocator* is he global address of documents, websites and other resources on the web.

VoIP:
V**oice-**O**ver-**IP, a category of hardware and software that allows you to use the Internet to make phone calls and send faxes instead of using the copper phone network. This technology is becoming very popular with businesses and home users alike because it greatly reduces telephone costs, both in terms of service and also phone system–related expenses. Often, VoIP phone services allows you to log in to an easy-to-use website to change the behavior of your phones, such as changing hold music or changing the hours that voice mail will pick up in the event of a holiday, etc.

VPN:
***V**irtual **P**rivate **N**etwork*, 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. Services like LogMeIn, GoToMyPC and others are in the same family but are not recommended for most businesses. In addition to often incurring an unnecessary expense, these services can expose your PC to the public Internet, which, even with a password, is a security risk. Your firewall typically will manage VPN connectivity.

VPN connectivity is also what allows two separate physical office locations to operate and access data on one network. If you have an office in your State and another in, another State the users in both offices can see the same files because the offices stay connected at all times via VPN.

Web Hosting:
An IT service that provides a home to your website and serves your website to people who visit your URL. Often, POP e-mail is included as part of a web hosting plan.

Wireless Access Point:
A network device that connects to your network via a network cable and broadcasts a wireless signal to mobile devices, tablets and iPads, and laptops. Often, multiple wireless access points will be deployed around the office (sometimes above ceiling tiles) to provide adequate coverage in all areas of the building.

An Invitation To The Reader

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

The technology industry is growing at such a rapid pace that most business owners can't keep up with all the latest whizbang 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 or less before they become obsolete. Sorting through this rapidly moving mess of information to formulate an intelligent plan for growing a business requires a professional who understands not only technology and how it works, but also 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 computer consultant. 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 in writing this book is not only to give you the information you need to find an honest, competent computer consultant, but in doing so to raise the standards and quality of services for all consultants in my 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 consultant, I want to hear those horror stories, as well. If you have additional tips and insights 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 my customers. I want to help business owners see the true competitive advantages technology can deliver to your 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.

Michael J. Servidio
Phone: (802) 865-4409
Info@tcivt.net
Technology Consultants, Inc.
589 Avenue D., Suite 30
Williston, Vermont 05495

FREE:
Confidential Cyber Security Risk Assessment Will Give You The Answers You Want, The Certainty You Need

($797 Value, Yours Free)

As a gift to those who have purchased this book, we are giving away a Free Cyber Security Risk Assessment. This is confidential, entirely free and without obligation.

What This Assessment Will Reveal:

- If your current IT company or team is truly securing your network and data; we'll give you a non-biased, qualified third-party review and truthfully provide you answers regarding security, backups and more.
- If your IT systems and data are truly secured from hackers, cybercriminals, ransomware and even sabotage by rogue employees.
- If your current backup would allow you to be up and running again fast if ransomware locked all your files – 99% of the computer networks we've reviewed failed this test.
- If your employees' login credentials and your own are being sold on the dark web right now and what to do about it. (I can practically guarantee they are, due to a recent 8.4 billion credentials being sold on the dark web. What we find will shock you.)

Here's How It Works:

We will have a brief, nontechnical conversation about your company's IT security and ask you a few questions you should be able to answer easily. Next, we'll conduct a quick, noninvasive, CONFIDENTIAL investigation of your computer network, backups and security protocols.

Your current IT company or team DOES NOT NEED TO KNOW we are conducting this assessment, or we can involve them. (The choice is yours, but we recommend NOT letting them know this inspection is happening so we can get a truer read of how secure you are. After all, cybercriminals won't tip you off that they're attacking.)

Your time investment is minimal: 30 minutes for the initial consultation and one hour in the second meeting to go over what we discover.

If we find problems, we will tell you what they are and prepare a Security Action Plan, for free, on how to remediate the situation; if you choose, we can assist you in its implementation.

After doing this for 40 years, I can practically guarantee I will find significant and preventable security loopholes in your network. Like Sherlock Holmes, we never fail. If nothing else, our Risk Assessment is an easy and cheap (free) way to get a valid third party to verify your security and give you peace of mind that you are protected.

How To Claim Your Free Assessment:

Go online to www.TCiVT.net/assessment.

Book Order Form

If you enjoyed this book and want to share it with others, we can provide discounted bulk purchases.

Quantity Discounts:

1 - 9 copies = $19.95 each

10 - 49 copies = $16.95 each

50 - 99 copies = $13.95 each

100 or more copies = Call for wholesale prices

Go Online To: www.TCiVT.net/bookorder

ABOUT
MICHAEL J. SERVIDIO

It is fitting that “Star Trek” launched Michael J. Servidio’s childhood interest in technology. Further encouraged by his brother, Richard, a structural engineer, Servidio was later encouraged to boldly go and start his own IT consulting company.

Servidio grew up in Middlebury, Vermont, which he describes as the quintessential New England town out of a Norman Rockwell painting. His father owned a plumbing company, and his mother was a switchboard receptionist for one of the largest department stores in NY City. Servidio’s science-minded brother, Richard, whom Michael calls “the kid who got to go to college,” gave his brother access to his computer, an Apple II, in 1979. Michael played games on the computer (yes, “Star Trek”), and Richard showed him how he would program the games.

Servidio initially entered the plumbing and heating industry and expanded into fire protection, installing sprinkler systems in high rises. In 1984, he went to work with Richard. His job was to assist with the drafting of plans for commercial projects, such as designing and drawing the steel frames to hold up all the water slides at Disney World’s Typhoon Lagoon. Richard did not like Michael’s handwriting and invested in a new desktop Computer-Aided Design program, the first in Vermont.

People took notice of how computers transformed Richard’s business. Servidio himself became an expert on this new technology and became a sought-after consultant. Richard urged him to start his own business. Servidio, wanting something steadier than the construction industry that he could do well and support his family, founded Technology Consultants, Inc. (TCI) with his wife’s support.

Focusing on small-to-medium-sized law firms, independent healthcare practices, and manufacturing companies, the former sprinkler systems designer now puts out IT fires, tailoring customized IT solutions to help businesses automate, scale, and grow. As a certified Microsoft engineer and seasoned consultant, Servidio has guided numerous small Vermont businesses into becoming multi-million-dollar enterprises through strategic automation and systems design.

Servidio’s mission is to empower clients to confidently navigate evolving compliance regulations while using compliance as a foundational driver of sustainable growth.

Over the past 10 years, Servidio has been a speaker and presenter at the Vermont Bar Association, Vermont Chamber of Commerce, and other meetings around the state. TCI donates to local charitable organizations, including COTS, which provides emergency shelter, services, and long-term housing for people who are experiencing homelessness and advocates for long-term solutions to end homelessness.

Servidio and his wife of 45 years have two daughters and five grandchildren. The family loves to spend time together in such outdoor activities as biking and kayaking. Disney World is the vacation destination of choice.

Servidio, like Captain Kirk, continues to explore new worlds in technology. Guiding his mission are several creeds that have served him for more than four decades: Do what you love, and it will never feel like work; forge partnerships with clients, do not be afraid to make mistakes; always be honest, even if it means losing a client; and help your competitor if they experience an emergency.