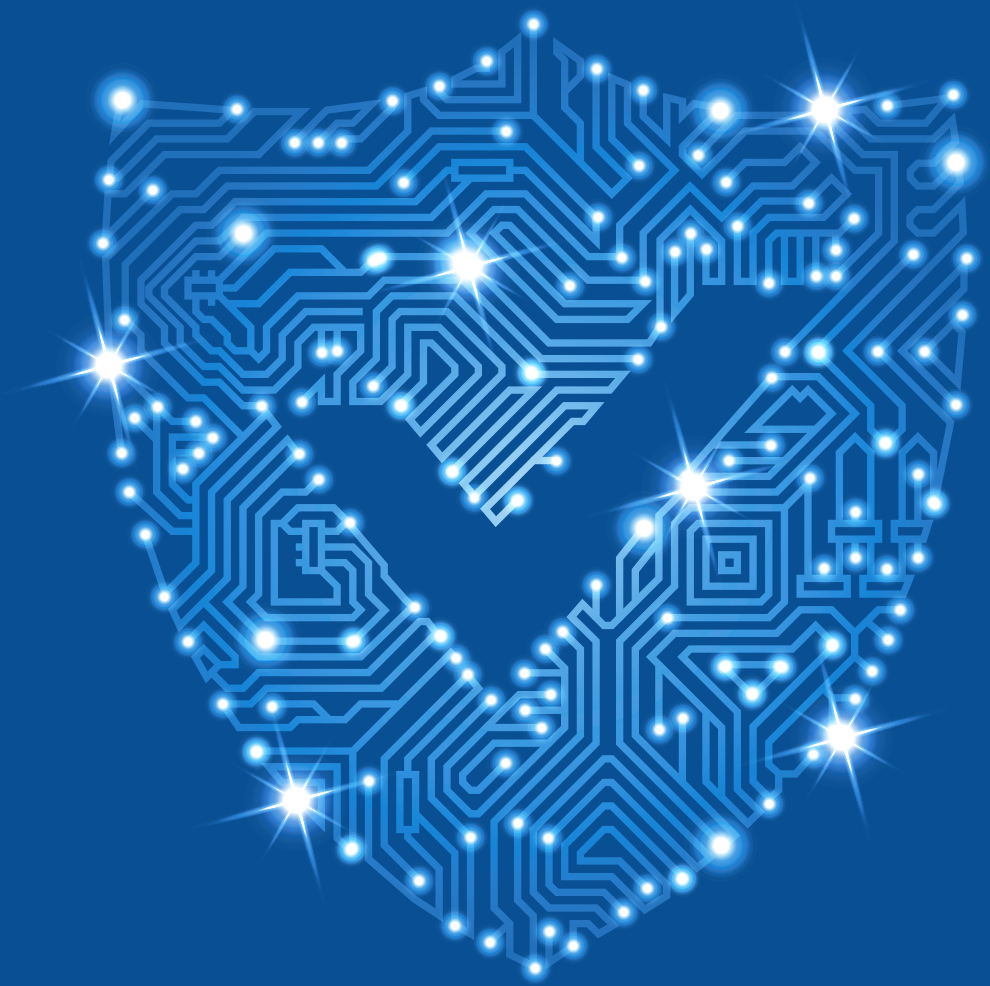
Cyber Defence 101: Choosing Your IT Partner

How to *Quality Check* an IT Service Provider
Before Letting Them into *Your* Business



Scott Birmingham C.E.T., C.I.M.

Principal Consultant, Birmingham Consulting Inc.

True Partnerships

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

- ✓ The scary truth about cybercrime and what you should be doing now to protect yourself.
- ✓ Critical questions to ask your next IT company to make sure their policies, procedures and protocols won't leave you stranded.
- ✓ The REAL cost of hiring a bad IT company or person.
- ✓ The most common mistakes made when choosing an IT company.
- ✓ 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.
- ✓ Everything you need to know about contracts, payment schedules and rate negotiations.

Principal Consultant For Birmingham Consulting: Scott Birmingham, C.E.T., C.I.M.

Cyber Defence 101: Choosing Your IT Partner

How to *Quality Check*
an IT Service Provider
Before Letting Them
Into Your Business

Scott Birmingham, C.E.T., C.I.M.
Birmingham Consulting Inc.
21 Mill St. N.
Waterdown, ON L0R 2H0
289-895-8948
www.birmingham.ca

Printed in Canada.

Publisher: Birmingham Consulting Inc.
21 Mill St. N.
Waterdown, ON L0R 2H0
www.birmingham.ca

Editor:
Brenda Jefferies, Freelance Editor

I dedicate this book to everyone who has ever been in the difficult position of having to make a complicated decision but feel like they don't have all the facts.

I hope this book helps with at least one of those decisions.

- Scott

Table Of Contents

Introduction

IT, Security, Compliance – What's the Difference?

I recently attended a security conference in which Bruce McCully, cyber security author and speaker, mentioned that he is frequently asked this question; so now he includes it in many of his presentations. Given that it's question we also often get asked, I thought I would borrow a page from his playbook.

To illustrate the difference, Bruce used a picture of a motorcyclist on what looked to be a very fast bike. The rider had an open backpack with a baby poking out of the top of the backpack – not strapped in and no protective gear on the baby. The bike and rider represented a business and the baby represented the valuable information the business depends on every day to function.

Just like a road trip, security is a journey. Using that analogy:

- IT's primary role is to get the baby there as quickly and efficiently as possible without any breakdowns.

- Security's primary role is to get the baby there safely: ensuring a proper baby seat, everyone has protective gear, and if it was a car, seatbelts and airbags are absolutely necessary.
- Compliance's role is to get the baby there without any tickets or fines (following, speed limits, obeying signs, stop lights, etc.)

All three are necessary to create the best opportunity for a successful trip. But even with all of these areas working together, there is no guarantee that the baby will arrive safely (motor vehicle mishaps are called *accidents* for a reason; and that's why services like CAA and car insurance exist).

The same holds true for your security journey. IT, security, and compliance all play a role in setting the stage for you to have a successful business journey. But just like road trips, there is always the risk of something unexpected happening.

A great first step in your business security journey is to ensure that your IT provider is in lockstep with you, so let's talk about picking the right IT partner.

IT: A Necessary Evil?

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

From email, 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 labour and paper using high tech – and that's a *good* thing.

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

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 many 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 large enterprises do. You're low-hanging fruit. Sure, they might not get $10 million from you, but they might get $100,000 or $500,000; and since there are far more small businesses out there than large corporations (by "small business" I mean less than 100 employees), many cyber criminals 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 $500,000 mistake, it's certainly not a good thing, but it represents only a minor blip in their overall IT budget. If a mid-sized business makes a similar 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 about who you take IT advice from, and why I wrote this book.

Very few business leaders 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 firm, you can free up your time and attention to focus on 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 tell you:

- ✓ The right questions to ask any IT company BEFORE you sign a contract. This is really, really important because you are handing over the "keys to the kingdom" to your IT 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", and overpriced IT services that don't deliver a return on your investment.
- ✓ How to avoid under-spending in critical areas like cyber security.
- ✓ What you need to know to make sure your data and your company are protected from an ever-growing list of threats, including ransomware, online criminals, faulty hardware and software, and even employee sabotage.

- ✓ 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 defence if your network is compromised and the authorities 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:
Why Listen to a Word I Have to Say?

This is a tough question. Usually, I like to be the one asking tough questions, not answering them. And if I were you, I'd also be thinking "Who is this guy anyway? Maybe I shouldn't listen to him."

To answer this question, let me take you back a few years…

I started my career designing automated control systems for large manufacturers like Ford, Kraft Foods, Magna International and Kellogg's.

At this level, downtime wasn't an option. I remember the very first project I did fresh out school in the early 1990s. It was for an automotive plant and I was told that when the line stopped, the cost was $5,000 per MINUTE – in 1990s dollars! (Not for the entire plant – only for that one line.) Just a little pressure for a new graduate.

I did projects at another plant where the downtime cost was $10,000 per minute because they had a higher-end product and faster line speed.

I learned early to over-engineer to account for any unknowns that crept up during a project, to set standards that were much higher than the bare minimum needed for things to function, and to build in contingencies and/or redundancies. I also learned the value of client service. If something did go badly wrong, understanding the impact to the business, the process, and the people involved, as well as having a sense of urgency to get it fixed made almost as much impact as fixing the problem.

I gleaned a lot more relevant knowledge from those early projects, but let's fast forward to the second half of the 1990s. I had the opportunity to open a branch office for an engineering firm, which involved setting up a server, the Internet connection, remote access to the main office, etc. This was the 1990s – things we take for granted now weren't so easy then.

It was this exercise that sparked my interest in IT. The problem was that most people in IT didn't think like I did. They lacked the sense of urgency, couldn't understand why something had to work 100% of the

time (surely, nothing could cost $10,000 a minute if it didn't work?!?), and couldn't be bothered to fix minor issues.

Again, some perspective: in my world then, downtime was measured in seconds. I recall having a conversation with a maintenance supervisor who asked for my help. He had been watching an assembly line and noticed that it seemed to slow down for a few seconds on a fairly consistent basis. He did some math and figured out that in a 20-hour production day, that barely noticeable slowdown was costing over $100,000 EVERY DAY. The problem had to be solved.

The IT people I met at that time would have balked at spending time on a problem like that with responses like, "It's barely noticeable. Don't worry about it. Live with it." Frustrating.

Fast forward a few more years to when I worked for a startup company also in the manufacturing space. I won't go into details, but the level of incompetence of IT people was beyond belief. I had yet to transition to IT, but I was forced into fixing problems that IT "professionals" couldn't. Some of the issues were the result of poor design choices they made, some were due simply to their inability to troubleshoot, and some

were caused by their inability to see outside their IT bubble.

It was at this point that it finally hit me. If I, as an engineering technologist, could apply the engineering methodology needed for manufacturing to the world of cyber security and IT, not only could I help more businesses, maybe, just maybe, I could raise the bar.

There's lots more to the story, but the bottom line is that in 2009, I left my job and took the plunge to establish Birmingham Consulting.

My team is pretty selective about whom we take on as clients, but over the years, we've helped dozens of businesses across many different industries: construction, logistics, recycling, healthcare, legal and professional services, to name a few.

Fast forward further to today and I see an almost identical pattern to what I saw in the 1990s/2000s when comparing automation engineering to IT. Only now, the pattern is with IT and cyber security. **The laissez-faire attitude that many IT firms have toward cyber threats is truly frightening.** Because of this complacency, you'll find cyber security as a primary theme through the following pages.

With that in mind, I'm passionate about educating and protecting business leaders. My hope with this book is that you will be able to make informed choices about whom to entrust with the security of your business.

If, after this little bit of information about me, you don't think I'm worth listening to, then stop reading and pass this book along to someone else.

On the other hand, if you think there is a chance of finding some useful information, I welcome you to continue. And at the end, there is an opportunity for you to provide feedback.

Chapter 2:
The True Cost of Bad Advice and Poor IT Service

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 leader can deny that IT problems cost money. If you've ever had your day grind to a screeching halt because the Internet went down, email 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 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 look at these statistics on the cost of IT-related downtime and disasters, as reported by various industry experts and studies:

- 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, cyber criminals 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 an 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 individuals in the past year – just in the**

U.S. And that doesn't include the hundreds of thousands of computers rendered useless by spyware. *(Source: Gartner Group)*

- Today, the average cost of IT downtime is over $5,600 per minute. This may sound like a lot, but when you factor in salespeople who can't 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 centre 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)*

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 client 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 incompetent firm 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) by 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, you 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 deadbolts and a home security system, complete with motion detectors, cameras and glass-break technology. Setting all of that up requires more work and means that your home will need 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 firm lacks experience in solving a problem, grossly underestimating the time and money it will take to successfully complete a project. When a firm 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 become 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 advice can cost:

- 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 of 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 can't just "unlock" your data. Someone has to comb through your files and devices to ensure the criminals 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!

- You'll need to handle the public relations nightmare that comes along with your employees' and clients' data being exposed via a breach, and you'll have to notify your clients that you exposed their data, credit cards, emails, etc., to criminals.
- You can be fined for non-compliance and data breach violations. Every jurisdiction 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 remember, private information isn't just medical records and financial data, but also email addresses, birthdays, social insurance numbers, mailing addresses, phone numbers and more. If you 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, wastes time and money, and you'll be forced to start over, *again*.
- Hiring a competent IT firm to fix what the other company messed up or complete the project you

originally planned (and paid for) means you end up paying double the cost.

- You'll end up paying in terms of time and money when the project you've paid big dollars for ends up being a solution that is too complicated and employees either can't actually use it or refuse to use it. (This happens with custom development all the time.)
- You'll incur litigation costs to get your money back from a company who failed to deliver on a contracted service.
- You'll be faced with the sheer frustration of dealing with 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 company, you've already invested a considerable amount of time and money, making it difficult, if not impossible, to end the project and look somewhere else.

Worse yet, when you do get breached, you'll be scrambling to find someone else to help you put all the

pieces back together again. You'll be forced to make another quick decision on whom to trust while under pressure, and you'll have 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 defence 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:
13 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 and unqualified technicians to 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

clients come to us to clean up the disasters they have caused. Occasionally, 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.

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 licence to practice? Would you want that person treating your illness or handling your tax return? Or an attorney who never

went to law school or passed the bar exam? Even truck drivers need training and a licence to operate. But, unfortunately, that's not 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 common mistakes to avoid when you're conducting that search:

- Mistake #1: Hiring an IT company that doesn't make cyber security their TOP priority. The old saying that the cobbler's children never have shoes is never an acceptable excuse for an IT company to have 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 #2: Choosing your next IT 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 service 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 with less than 100 employees, they might not really want you either, and they'll give their best techs and services to larger organizations with bigger budgets.

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

- Mistake #3: 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 #4: 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 whether their 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 #5: Locking in for 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 our business, we allow six months to work with a new client and get to know each other. After that, if either one of us feels like it isn't working, we can end the relationship with no penalty.

- Mistake #6: Hiring an IT firm before you've spoken directly with three to five of their long-term current clients who are in industries 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 #7: Hiring an IT company that doesn't insist on doing an assessment of some kind BEFORE they provide you a full proposal 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).

Some firms charge for this service while others do it for free. It's your choice if you're willing to pay for the assessment, but I would expect a much better analysis from someone who is getting paid to do it. Remember the adage that "you get what you pay for".

- Mistake #8: Hiring an IT firm with limited cloud experience. Many veteran technology consultants are stuck in the past and haven't kept up with the industry. Their ideal scenarios continue to be physical servers and equipment inside your office as the only way to do things.

  Sometimes the "on-premise" approach is still the best option, but more and more frequently, newer cloud technologies such as Microsoft 365, Amazon Web Services and Microsoft Azure, are capable of delivering the same, or even better, solutions with less cost, more flexibility and better security.

A *good* consultant will understand cloud technologies and offer them as an option, either fully cloud-based or a hybrid solution of cloud and on-premise equipment.

A *great* consultant will go a step further and determine what options provide the best return on investment, the options that best align with the longer-term goals of your business, and a solution that fits the overall vision you have for the company.

- Mistake #9: Hiring a firm 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 favour or "saving you money".

- Mistake #10: Hiring 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 the 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.

- Mistake #11: Being someone's test subject because they are providing a solution they've never implemented. I'm not suggesting that you should only hire a firm that knows everything there is to know about IT – that's simply not possible because the world of technology is in a constant state of flux. There is

a fine balance between fully understanding a particular technology and that technology becoming obsolete.

What I'm talking about are the fundamentals. If you hire a firm to implement the latest version of a solution, it might be the first time they've implemented that particular version BUT they've implemented previous versions or similar systems for other clients. This scenario is common and expected.

On the other hand, if they have no experience with a particular solution that they're recommending, let them learn with someone else. For example, if you need a VoIP phone system, don't hire a firm for whom you would be their first VoIP client.

- Mistake #12: Choosing to not make a decision. An event or series of events led you to investigate and evaluate alternate IT firms. But change is hard. It can be disruptive, and the pain of change could be worse than the pain of staying with the status quo. People concerned about the pain of change will often decide not

to choose a new provider. As the saying goes “a bird in the hand…”

If you find yourself in this situation, I encourage you to heed the words first spoken by psychologist William James: “No decision is a decision” – don’t decide to simply live with the issues that prompted your investigation. At least bring them to the attention of your current provider to get them resolved (if you haven’t already), and put the information in this book to use by asking them some of the questions.

- Mistake #13: Did I mention hiring an IT company that doesn’t make cyber security their TOP priority? I can’t stress this enough. Too many businesses AND IT firms don’t truly understand just how critical cyber security is.

Chapter 4:
25 Critical Questions That Reveal if the IT Service 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 that their answers are included IN WRITING in the contract. They might

say they offer after-hours service but may have a carve-out in their agreement stating that it costs extra, or the response time isn't guaranteed.

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

General Business and 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 into a portal to submit a ticket and won't allow you to call or email them. This is for THEIR convenience, not yours. What do you do if the Internet is down or you can't log into 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.

Also, ask what ticketing system they use. If they use a "homegrown" system, that is a RED FLAG. Chances are they are tracking time and activities manually and lack integration between ticketing, scheduling, project management and billing. There are lots of ticketing systems available for IT firms ranging in cost from free (but almost useless) to expensive (but with a lot of functionality and flexibility to adapt to specific client needs).

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

Q2: What is your support process?

I'm sure you've been frustrated with customer support for large technology companies – maybe your Internet provider or phone company, a large computer manufacturer, software vendor, etc. You know the drill:

the person that you first talk to follows a pre-defined script of steps to help you – most of the time, the steps aren't even related to the problem you're trying to solve!

When that person finally gives up, they refer you to someone more senior and you start the process all over again. Even though the first person supposedly informed the next person about your problems and what had been tried to resolve it, often the second person repeats the same questions and same steps before trying something different.

Then if person #2 can't fix your problem, you get bumped to person #3. By the time you finally get the problem solved, it's taken way more time than it should have.

You might ask yourself why is it that every large corporation seems to have the same horrible support model? Well, there is actually a reason: there is a defined standard for this tiered support model and most large companies follow it. To compound things, companies consider "tier 1" to be a junior role and hire accordingly.

A client-focused IT firm understands how outdated and broken this tiered model is and will have a better process in place.

In our business, "help desk" is actually a senior position, not a junior role. The goal is for the first technical resource our client speaks to own the issue and solve the problem.

Q3: Do you offer after-hours support and if so, how does it work?

Any good IT company will answer their phones live and respond to your calls during business hours. But they should also have the ability to provide support outside of their regular business hours.

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 after-hours support and understand what the costs will be.

Q4: Do you have a written, guaranteed response time to working on resolving problems?

The industry term often used for this metric is "Service Level Agreement" (SLA).

This question needs to be asked, but the reality is that it's a TRICK question for you to ask and see how they respond.

A lot (and I mean A LOT) of IT firms focus on this metric as the holy grail of IT service and most IT firms will respond with time frames for things like first response, technician assigned, work started, time to resolve, etc.

The reality is that if the IT firm is doing their job properly, the importance of SLAs diminishes significantly because problems will be fewer and far between.

The more important question is whether they prioritize by severity. A network outage had better take higher priority and have a faster response than helping someone re-create the email signature they accidentally deleted.

The answer to this question will help you determine if they are truly proactive or if they are, in

reality, reactive. SLAs are extremely important for reactive companies.

When it comes to SLAs, the best response from an IT firm to a potential client that I've ever heard is, "Our SLA is that if you aren't happy with our performance, you fire us."

Q5: 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).

Q6: How much errors and omissions (E&O) and general commercial liability 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, or to lose data, 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 errors and omissions insurance and workers' compensation insurance – and don't be shy about asking them to send you the policy to review!

True story: a few years ago, a company that shall not be named was slapped with several multimillion-dollar lawsuits from customers for bad behaviour by their technicians. In some cases, their techs were accessing, copying and distributing personal information they gained access to on customers'

computers 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.

Q7: Tell me about a time when you made a mistake that impacted a client and how you handled it.

Sounds like the type of question you would ask during a hiring interview, doesn't it? Well, it should. How they respond and how they handle the question speaks to their integrity.

If they can't provide you with an example, it should be a big red flag. Every IT firm in existence (including ours) has made mistakes. Do they own their mistakes, cover them up, or shift blame to either a supplier or a piece of equipment? If they owned a mistake, how did they communicate with the client and deal with any fallout?

I'll share a real-world example of what I'm referring to. One afternoon, we started getting reports from a client about email problems for a large number of users. It's important to note that email had been

functioning for a long time – this was a sudden inexplicable problem.

We jumped on it, found a misconfigured setting and corrected it quickly to get the client functional again. I called the client to confirm they were up and running again.

Now it was time to find out why this setting had randomly changed. We determined that one of our techs inadvertently changed the setting when he was working on another ticket. To say I was not happy was an understatement.

I could have told the client that it was a mystery, and we would keep an eye on things (unfortunately, this is sometimes the case because large software companies sometimes push out changes that break things). Or I could have blamed the company hosting their email, or tried some other way to avoid taking responsibility – after all, who would know?

Instead, I immediately retrieved the key to the client's office and drove there. I met with both the president and vice president. They weren't expecting to see me, but they made time for me. I let them know that one of our techs had inadvertently caused the

email problem and apologized. I then pulled their office key out of my pocket, placed it on the boardroom table, and continued by saying that I completely understood if this mistake meant the end of our relationship.

They were dumbfounded. Literally speechless. There was one of those awkward silent pauses before they accepted my apology and told me to put the key back in my pocket. That was more than five years ago and they are still a client today.

IT Maintenance (Managed Services):

Q8: Do you offer true managed IT services and support?

As mentioned earlier, you want to find an IT company that will:

- Proactively monitor for problems.
- Proactively correct any problems found before they affect you and your staff.
- 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.

Q9: How do you define "proactive"?

We've seen widely varying answers to this question. One company responded that receiving alerts showed they were being proactive – they made no mention of actually responding to the alerts. Another stated that they recommended old equipment be replaced before it failed – it doesn't take a genius to figure that out!

A truly proactive IT firm will:

- Not only monitor for alerts, but will also respond to them before you even know there's a problem.
- Assess your systems on a scheduled basis to identify POTENTIAL problems and deal with them so that you never see it.
- Prepare a scheduled and predictable equipment refresh plan so that you aren't caught off-guard.
- Understand your business plan and cycles so that they can ensure that you have the right

technology at the right time and aren't forced to play catch-up.

When an IT firm is truly proactive, business leaders sometimes feel like they are paying too much for IT because they mistakenly equate value with how quickly the phone is answered and how fast a problem is responded to instead of how smoothly their IT runs.

Value should not be based on how great an IT company is at *reacting*. If you could pay the same amount for either a great reactive company that you interact with frequently and who fixes problems quickly, or a proactive company with whom you interact less frequently because there weren't any problems, which would you prefer?

Q10: 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 cloud migration, 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 and Google Workspace?

- 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 even if it's out of the scope of the contract. Clarify this up front.
- What about on-site support calls? Or support to remote offices?
- If our employees had to work remotely (due to a pandemic, shutdown, natural disaster, etc.), would you provide support on their home computers 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.

Q11: Is your help desk internal 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 third party on the history of your account.

Q12: How many *technical* resources do you have on staff?

Be careful about hiring small, one-person-shops or 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.

Q13: 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 an ongoing basis.

Why is this important? There are several reasons. First, it shows professionalism and integrity in protecting YOU. No single 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 of your systems.

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 to find things and uncover accounts, hardware, software licences, 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, good documentation will enable your replacement company to take over quicky.

Side Note: If your current IT 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.

Q14: Do you meet with your clients regularly as part of your managed services agreement?

Professional firms will offer to meet with you at least annually (sometimes more often) to provide a "technology business 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 any future plans for expansion or 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.

Q15: If I need or want to cancel my service with you, how does that happen and how do you offboard us?

Make sure you carefully review the cancellation clause in your agreement. Some 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.

But keep in mind that cancellation fees or penalties are not the same as offboarding costs.

Just like onboarding, offboarding is a mini project. If projects are outside of the agreement, then you can expect a bill. If it is excluded, be sure to have this

included in the agreement as a fixed amount so that you avoid widely varying costs.

Cyber Security:

Q16: Tell me about the cyber security practices you use in-house.

The key thing to understand is whether they "practice what they preach". Have they implemented the same security measures they're recommending for you? If not, why not? The right answer is that their practices will at MINIMUM match the highest level of security they provide for clients. The best answer is that they are doing even more.

A good IT firm will be paranoid about their own cyber security because they understand if they are breached, there is a high probability that all of their clients will be breached as a result.

Q17: How do you protect our employees' devices to ensure they're not compromising our network?

The answer to this question may get a bit technical. The key is that they HAVE an answer, and don't

hesitate to provide it. Some things they should mention are:

- 2FA (two-factor authentication).
- Advanced end-point protection, NOT just antivirus.
- Limited local administrative rights.
- Ransomware detection and automatic process kill.
- At least one advanced email threat protection application (two layers of advanced protection is preferred), not just built-in spam filtering.
- Internet content filtering to prevent access to harmful websites.

Q18: Aside from traditional E&O, how much cyber liability insurance do you carry to protect me?

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 due to business interruption, they might not be

able to pay and you'll 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.

Cyber liability insurance is becoming insanely expensive compared to other types of insurance. It's even worse for anyone in the tech sector, specifically IT firms. Cyber criminals know that if they can compromise an IT firm, they have access to dozens or hundreds of other companies.

Insurance companies are tired of paying for all of the costs associated with breaches and are starting to refuse new cyber liability business. In addition, they are either denying renewals or significantly increasing rates while also imposing stricter conditions to get approved for coverage.

This is not only going to change the insurance landscape for every business, but it's also going to completely disrupt the IT industry because small players will no longer be able to afford cyber liability insurance.

The situation is akin to what happened with snow plowing a few years ago. Snow removal companies get sued by people who injure themselves by slipping or falling in winter conditions. Insurance companies for snow removal companies were tired of the large payouts. So they increased the insurance for any company in the "snow management" space.

As a result, the entire snow industry changed. Small players disappeared because they couldn't afford the new insurance costs, and the price paid by property owners to snow removal companies increased dramatically.

Find out if the IT firm can provide proof of cyber liability insurance in case your own cyber liability insurer needs it.

Q19: 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 an annual 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.

Q20: 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 centre, is a centralized department within a company that monitors and deals 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.

Q21: Do you have a written Incident Response Plan (IRP) and written procedures to respond to a ransomware attack? Can I see it?

Dealing with a disruptive cyber attack will most likely involve law enforcement and insurance companies. Not having a written procedure to follow in a high-stress situation can lead to mistakes and a lack of evidence for law enforcement and the insurer. Part of being proactive is planning ahead for these types of situations.

But what about less disruptive “incidents”? What if a laptop is stolen or lost? Does the IT firm have steps in place for “routine” incidents?

Q22: 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. 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 IT firms that have been caused at the vendor level, not due to the fault of the IT firm.

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 definite warning signs you don't want to ignore.

Backups and Disaster Recovery:

Q23: Can you provide a timeline of how long it will take to get our 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 home or to a service station where you can fail back to a new or repaired tire.

In the event of a disaster that wipes out your data and network, be it a ransomware attack or a natural disaster, you will 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. There should be two fail over options: local in your facility and replicated in the cloud.

All backups need to be locked down separately to prevent ransomware from infecting the backups as well as the physical servers and workstations. If their backup solution uses software on computers that can

be run by someone using that computer, it's not secure.

At some point, you need to fail back to your main network and/or servers – 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 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 and timeline for restoring your network and data.

In this day and age, regardless of natural disaster, equipment failure or any other issue, your critical business systems should fail over immediately (i.e., less than an hour) with full fail over within six to eight hours (or less).

Q24: Do you INSIST on doing periodic test restores of our backups to make sure the data is not corrupt and could be restored in the event of a disaster?

A great IT firm 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, one is a week old, and the other 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.

Q25: If we were to experience a location disaster, pandemic shutdown or other disaster that prevented us from being in the office, how would you enable us and our employees to work from a remote location?

If 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 remotely (and securely, I might add) when COVID shut everything down. Ask to talk to a few of their clients about how the process went.

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 appropriately?

Do their personnel present themselves as true professionals when they are in your office?

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 can't 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 and 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 bring more experience to the table than a generalist.

Do they keep the skills of their technical team up to date?

The world of IT is constantly changing, and it can be difficult to keep up. Good IT firms recognize this and will foster an internal culture of continuous learning.

If you hear that an IT firm is too busy to keep up with industry changes and trends, that should be a red flag. Don't misunderstand me – you don't want someone who is always trying to deploy the latest new thing. By the same token, a company with techs living in the IT Stone Age means that you won't get the productivity from technology that you need.

The right balance is for a firm to be solid in current technology, has learned from the past, and keeps an eye on the future so they can ensure your business needs are met.

How do they decide to recommend and roll out new technology to clients?

Do they test new technology and changes/upgrades internally before recommending and installing them for clients? Or are clients their guinea pigs for new things?

Do they "eat their own dog food" by using the same solutions in-house that they recommend to you? Often, this is not the case. Solution A will be used in-house because it's less expensive than identical

Solution B; but they sell Solution B to clients or vice versa.

If an IT firm is not willing to use the same solutions they recommend to clients, it begs the question, “If this solution is so good that your clients should use it, why don’t you use it in-house?” There could be valid business or technical reasons for using something different in-house, but you need to be comfortable with their answer.

The True SuperSTAR IT Firm You Want vs. A Self-Declared SuperSTAR	
True SuperSTAR	**Self-Declared SuperSTAR**
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, cyber liability 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
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
Has an established office	Has no office, uses a P.O. box and a cell phone, works from home

The True SuperSTAR IT Firm You Want vs. A Self-Declared SuperSTAR	
True SuperSTAR	**Self-Declared SuperSTAR**
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, 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 client satisfaction	Is apathetic toward problem resolution, has no policies or procedures for resolving problems

Chapter 5: Options for Getting the IT Service You Need

When you think about IT support for your business, not only are there different ways to approach it, but there are also a lot of different IT companies to choose from. But which approach 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 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, client 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, emails 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 businesses 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 that you're pulling these people away from the main job you hired them to do. And unless they have the time to stay up to date on the latest developments in IT and cyber security, 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 neighbour'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 team to support your network, but there are limitations you need to be aware of.

First of all, a single person can know everything there is to know about IT 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 through the duds 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 support don't provide the best return on investment for the average small to mid-sized business; and typically doesn't make sense until you have closer to 100 employees. There are certainly times when it makes sense to hire internal IT staff. For example, when you need specialized skills for application development and support. But often it doesn't makes sense for day-to-day IT support and maintenance.

Option #4: Use the IT support offered by your Internet Service Provider (ISP) or other big-tech vendors.

A number of big-tech companies, like Canon, Dell, Bell, Kyocera, Apple, HP, Xerox (the list goes on), 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.

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

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 North American 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 person 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: Add IT support to the same company that installed your phone system, video surveillance system, photocopier or other related service.

One of the trends with tech is the convergence of related technologies that share some overlap. Voice phone systems, video and physical security systems are prominent examples – some of them have completely migrated to network and cloud technology and some simply require some element of IT to function.

The best example is voice phone systems. As voice technology migrated from traditional analogue phone lines with a central system in your office (think Nortel phones with multiple incoming Bell phone numbers) to VoIP technology where calls are made over the Internet, companies who sold and serviced traditional voice phone systems saw their business fading away.

Their solution was simply to start selling and servicing these newfangled VoIP phone systems. The problem is that the technology is vastly different between analogue technology and VoIP. Nonetheless, once they've implemented some VoIP systems, these companies decide that they are now IT experts and convince businesses to outsource IT to them. Big mistake. Huge.

Let me share with you a real-world example. We were approached by a potential client during COVID who was looking to change IT service providers. I learned that they were evaluating our company and a phone-first company like the one I described above.

We were informed that the phone-first company was selected. They were about half the price we proposed. Fair enough – we shook hands (virtually) and parted as friends. Remember this was during COVID.

About two months later, we received an email from them indicating that they wanted to re-engage with us. When I asked the reason, they informed me that the phone-first company didn't "ask the right questions" and it became obvious that they really didn't have an

in-depth understanding of IT systems, networks, cyber security, etc. That prospective client became an actual client soon after.

Option #6: 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 and mid-sized 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 years, so I have considerable experience working with – and talking to – other businesses and IT firms. I've seen the horror stories and heard the complaints businesses have with other technology service vendors. I've worked with the 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 IT people they'd been working with. Based on that experience, I think the best option for a small to mid-

sized 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's the way we've modeled our company, and we've been able to deliver consistent, professional services to dozens of businesses in Southern Ontario.

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-sized 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?

One of the most common 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 $70 per hour but puts a junior tech on the job, the tech might take three hours to do something that another company would charge $100 per hour for but completes in 30 minutes. Then, of course, there's the question of whether 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 favour and can lead to you 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 computers 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. It's a very common model, and the companies offering it 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, additions and changes to your network to be billed on top of the monthly fee.

TaaS. Some IT firms sell their services using a "technology as a service" model (TaaS), 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 without having large lump-sum costs for hardware refreshes or software upgrades. 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 a heavy cash outlay for hardware and software if you need it. The downside is that, over time, you'll pay 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 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 don't 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, positively 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 email 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 a Consultant's Favour, Not Yours

Under a break-fix model, there is a fundamental conflict of interest 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 client. 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 client, 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 or how long it should take to resolve a problem, 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 of dollars the next.

So, What IS a Fair Price?

Most IT services companies selling break-fix services charge between $70 and $250 per hour, with a one-hour minimum. In most cases, they will give you a discount of between 5% and 25% 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 computer for a new employee. If you are hiring an IT consulting firm for a project, I suggest you demand the following:

- A detailed scope of work that specifies what "success" is. Make sure you detail what your expectations are regarding 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 miscommunication and additional fees later, and ensuring you get what you REALLY want.
- 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. In the 1990s and early 2000s, this was based on the number of company-owned computers, servers and network equipment that needed to be maintained, backed up and supported (i.e., per-device). But with the explosion of devices used in business settings and with employees using their own cell phones, tablets, and sometimes their own laptops (known as “Bring Your Own Device”, or BYOD), this per-device model became outdated.

So then, MSPs started pricing per-user (sometimes referred to as “seats”), regardless of the number of devices. But even this model is growing outdated as IT environments become more complicated with in-office, cloud, remote, BYOD, etc.

By far the best approach is to not price per-anything; but to base it on the overall environment. IT environments are complex and can be somewhat fluid due to some things beyond the control of your business or the IT firm (e.g., George drops his personal phone on a weekend excursion and buys a new one; Monday

morning, he needs all his work stuff set up on the new phone).

It also makes staffing changes MUCH easier. For example, someone leaves this week but a finding replacement takes six weeks; or an additional employee is hired but someone else leaves four months later. Adjusting the contract every month can be arduous for both parties. Having a fixed monthly fee that is reviewed by both parties on a scheduled basis makes it a win-win. Regularly scheduled Technology Business Reviews (TBRs) are a great time to have this discussion.

Unfortunately, many MSPs have not kept up with this changing business environment and still quote per device or per user. This means that when your best salesperson decides they need a tablet in addition to the laptop, desktop and mobile phone they already have, your monthly bill could change.

The other caution is that “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, you can't assume that a company that charges $3,000 per month is automatically cheaper than one that offers managed services for $5,000 per month 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 recovery from a ransomware attack – 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. Conversely, using 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 Service 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 negligent…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 cybercrime where client or patient data is compromised, you will NOT get such sympathy. Most likely, you will be instantly labeled "negligent" 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 and face serious fines and lawsuits EVEN IF you trusted an outsourced IT support company to protect you. Claiming ignorance is not an acceptable defence, and this giant, expensive and reputation-destroying nightmare will land squarely on YOUR shoulders. But it doesn't end there…

According to provincial and federal legislation, 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 may not 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 businesses stubbornly insist, "That won't happen to us," or, "I'm too small…nobody wants access to our data." They 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 Cyber Security 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 or data-breach fines. And in some instances, they simply want to "save face".

In fact, the National Cyber Security 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 criminal 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 over $100,000 and over 25 hours of downtime per ransomware incident. 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 criminals 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. Or them might retain access to cloud applications such as social media sites and file-sharing sites (e.g., Dropbox or OneDrive) – accounts your IT department may not know about or simply forgot to change the password.

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 cheque and credit card fraud, your hard-earned money can easily be stolen over time in small amounts that you simply never catch or discover.

Further, if your IT partner is not monitoring what is going on, employees could do things that put you in legal jeopardy, like downloading illegal 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 emails 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 and work Towards Cyber Liability Insurance Compliance

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 to ensure that their efforts aren't compromised or circumvented by your employees, or that you're not 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 can't 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 that it's something that's actually necessary, not just 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 clicking, unsuspecting, on a shared Google Docs link in an email, 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 emails and links, and downloading files that can circumvent security protocols and infect your network.

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

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 your business.

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 defence against being 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 contract; 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 you must be sure to 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 will you be charged for it 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, along with payment for any hardware or software purchases up front. However, you should never pay a consultant in full before a project is started, and you should not be asked to pay the balance of a project until it is completed to your satisfaction.

As a rule of thumb, try to reserve 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.

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 each. 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; 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 following:

- 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)

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. A word of caution here: some

will even offer to custom-build your server and workstations instead of purchasing a name brand. DON'T DO THIS! We've been brought in to fix these nightmares – everything from incorrectly assembled interior components to the builder refusing to warranty a failed component.

Stick to trusted name brands like Dell, Lenovo, or HP. And be sure that you will be getting business-grade equipment with three years of warranty and accidental damage protection.

Another true story: we used to only add accidental damage protection to portable devices like laptops so that damage from drops or spilled coffee would be covered. That was until a client did an office rearrangement over a weekend and dropped a brand new all-in-one computer during the shuffle. No warranty protection for that! Since then, every laptop AND desktop computer we purchase for clients includes three years of accidental damage protection. It adds to the price, but you'll be glad you made the extra investment.

Also, you want to keep in mind that your IT firm is probably not making a lot of money on selling

equipment 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? Some IT firms 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 and be prepared for it to affect the price.

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 (during or outside of 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 firm 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 get confirmation that your notice of cancellation was actually received. You don't want an email to go missing, rely on a phone call or have an actual written letter get lost by the post office.

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 common outsourced function for businesses of all sizes is IT.

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 can't be pushed on to an individual IT person or team that lacks the deep knowledge, tools and expertise required. Another example would be the cloud migration of a critical business system.

- 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; finding a good IT person of any calibre is difficult. Then you have to consider a "Plan B" if they leave or are suddenly unable to work. If you don't have backup person who knows your systems, you can go through a VERY painful period trying to hobble along until you replace them. This is why many of our larger clients who HAVE internal IT choose our CoMITS, short for co-managed IT services (more on this later).

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

With 75 or more technology users, it may make sense to have an IT person on staff, depending on the unique needs of your organization. But often that person 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.

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-user 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 patient and client 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 defence to troubleshoot end-users' problems, questions and needs. Needs to be highly responsive.	1 per 70 employees	$50,000 - $70,000
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	$70,000 - $90,000
Network/ Systems Engineer	Responsible for the strategic planning and implementation of the communication networks in your company.	1 per 200 employees	$70,000 - $90,000
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	$150,000 - $200,000
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			$615,000 - $850,000

*Salaries vary by region, city and relevance/depth of experience.

It's important to keep in mind that most businesses will not need the above individuals' expertise 24/7/365 (e.g. the CIO and 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 tools
- Business Continuity and Disaster Recovery (BCDR) services
- Cyber resilience tools like advanced endpoint protection and advanced network protection
- Managed Detection and Response (MDR) provided by a Security Operations Centre
- Vulnerability assessments (nobody should check their own work)
- And many more

The list could get lengthy, depending on what you currently have in-house and your specific business needs, but you get the idea.

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 services, or CoMITS for short.

Co-managed IT gives companies the helping hands, specialized expertise, 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 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 internal team behind to try and support it.

- 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 parental

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 would require 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 which 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. Also, 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 IT staff is better utilized by working on high-level strategic projects, but they need 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.

Scenarios Where Co-Managed IT is NOT the Answer

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 can't get beyond this concern and will dig in their

heels 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 aren't open to a new way of doing things.

  This point is closely tied to the previous point.

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

However, a big value we bring to the table is our combined years of expertise in supporting and securing computer networks. Therefore, the clients we get the best results for are those who are open to 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 can't take on a client who 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" – there is simply too much liability for us.

- 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. 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

Advanced Endpoint Protection (AEP):

Advanced endpoint protection refers to the category of security products that has emerged in response to the inability of traditional antivirus to detect and block unknown malware and exploits. AEP protects servers and computers from malicious software, especially these previously unknown threats, by using machine-learning or behavioural analysis. Traditional, reactive security tools such as antivirus software generally depend upon known threat information to detect attacks.

Amazon Web Services (AWS):

AWS is the world's most comprehensive and broadly adopted cloud service. It offers database storage, resources to run software in the cloud and

hundreds of other services that used to require the purchase and maintenance of expensive hardware in your office. Primarily used by software companies to host and run the software they provide to their customers, AWS offers businesses the ability to pay for computing resources based on consumption, much like a utility.

Antivirus Software (Traditional):

Antivirus software is a security program designed to monitor a computer, server, tablet or phone for malicious software. Once detected, the software will attempt to remove the offending item from the system or, if it is unable to remove the malicious program, it may simply quarantine the file for further analysis by a network administrator. Because antivirus software depends on a list of known threats to find malware, it's crucial to keep the software up-to-date at all times so that as new threats are identified, the software knows about them.

Business Continuity and Disaster Recovery (BCDR) Appliance:

A “BCDR” appliance is a device used to back up your servers and data, which drastically reduces recovery time should the actual server have a problem. Unlike other backup technology, such as File and Folder Backup, a BCDR appliance can step in and perform the role(s) of your server(s) so that your employees can continue to work.

A BCDR reduces recovery time from days to hours because instead of backing up individual files, it takes a “snapshot” or picture of the entire server, including all operating system and program files (i.e. an “image-based backup”).

Typically, a BCDR performs a backup once per hour, so you should never lose more than an hour or two of information. It also automatically stores the backups offsite, which gives you the ability to “turn your server back on” from the last successful backup in the event of a physical disaster, such as a power outage, fire, hurricane or flood.

Cloud Computing:

This is a general term to describe “Internet-based” computing, where shared resources, software and information are provided to your computer, phone, tablet and other devices on demand via the Internet. Facebook, Google Search, Microsoft 365, Gmail, QuickBooks Online and similar services are all examples of cloud computing services.

Cloud computing, such as Microsoft Azure or Amazon Web Services (AWS), also provides a means for you to have a server for your business that isn’t inside your office or building. It offers the same functionality and features that previously required businesses to purchase, power, and maintain expensive hardware on site.

Content Filtering:

Content filtering prevents users from accessing or sending objectionable content via your network. Although this usually refers to web content, some programs also screen inbound and outbound emails for offensive and confidential information. Note,

content filtering software is different from antivirus and AEP.

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

Cyber Attack:

Any attempt to bypass the security of an IT environment or device. An attack can focus on gathering information, damaging business processes, exploiting flaws, monitoring targets, interrupting business tasks, extracting value, causing damage to logical or physical assets or using system resources to support attacks against other targets. Cyber attacks can be initiated through exploitation of a software or device vulnerability, through tricking a user into opening an infectious attachment, or even causing automated installation of exploitation tools through innocent website visits.

Cyber Resilience:

Using the philosophy of not “if” but “when” a breach will occur, cyber security has evolved from only focusing on prevention to a more holistic view that includes mitigation and recovery. In other words, how “resilient” is your business to withstanding a cyber security incident?

Cyber Security:

Cyber security refers to the processes that safeguard and secure the storage and sharing of information within an organization from being stolen or attacked. It requires extensive knowledge of the possible threats, such as cyber crime, viruses and ransomware. Identity management, risk management and incident management form the crux of cyber security strategies within an organization.

You may hear security professionals using the broader term “information security” instead of “cyber security”. However, for most people, the terms are used interchangeably. As an analogy, “cyber security” referring to “information security” can be likened to

the band name “Kleenex®”, which is often used as a catchall for the broader term “facial tissue”.

Cyber Security Incident:

A cyber security incident is an unplanned disruption or degradation of a network or system and needs to be resolved immediately. An example of a cyber security incident is when an employee’s email account is accessed by an unauthorized person. However, if the disruption is planned, such as scheduled maintenance, it is not considered a cyber security incident.

Data Breach:

A data breach is the disclosure of, or access to, private information; destruction of data; or abusive use of an organization’s private data either by the malicious act of a third party or the mistaken action of an employee. Generally, a data breach results in private data being made accessible to an unauthorized external entity. For example, if an employee’s email account is accessed by an unauthorized person, not

only is it a cyber security incident, it's also a data breach.

Data Centre:

A data centre is a physical facility used by organizations to store and run their critical data and/or applications. Data centres provide a network of physical servers and storage and allow businesses to either rent space to install their own equipment or the option to pay a monthly fee to use equipment owned and maintained by the data centre.

Dynamic Host Configuration Protocol (DHCP):

DHCP relates to how computers and devices on your network receive the IP address used to communicate with each other. Much like street addresses, devices have an address on the network. This is how your computer knows which office printer or copier you want to send your document to. IP addresses can be assigned either statically or obtained automatically (i.e., dynamically). When a device receives an IP address automatically, it's called DHCP.

Your computer's network IP address is typically assigned by DHCP.

Disaster Recovery Planning (DRP)

A disaster recovery plan (DRP) or a business continuity plan (BCP) details the steps required to restore critical business processes in the event of a disaster. Disaster recovery planning aims to bring business activities back to normalcy in the shortest possible time. Creating a disaster recovery plan requires an in-depth study and analysis of business-critical processes and their continuity needs. Business continuity plans also prescribe preventive measures to avoid disasters in the first place.

Domain Name System (DNS):

DNS is an Internet service that translates domain names into IP addresses. Think of it the global Internet directory.

Even though most domain names are alphanumeric, devices can only communicate with an IP address. When you enter www.microsoft.com into

your web browser, the browser uses DNS to look up the corresponding IP address. Same thing when sending an email to someone@business.com: your email server uses DNS to look up the IP address of the business.com email server. As a simple example, when you browse to www.google.com, DNS tells your device it can be found at IP address 74.121.78.241.

Domain:

A technology used in Microsoft Windows Server operating systems to manage computers and user accounts, including who has access to what.

Domain Name:

The identifier of your business that works in conjunction with DNS for your business to be found on the Internet. Your domain name is used to locate your website and us also the portion after the "@" sign in your email address, such as yourname@yourbusiness.com.

Encryption:

Encryption is the process of maintaining data integrity and confidentiality from unauthorized access. Encryption converts data into a secret code with the help of an algorithm. Only authorized users with an encryption key can access encrypted data.

Endpoint Detection and Response (EDR):

Endpoint detection and response is a device-based security solution that combines real-time monitoring and collection of information with rules-based automated response and analysis. EDR is an emerging security solution that detects and investigates suspicious activities on servers and computers, employing a high degree of automation to enable security teams to quickly identify and respond to threats.

The primary functions of EDR security are to monitor and collect activity that could indicate a threat, analyze this data to identify threat patterns, automatically respond to identified threats to remove or contain them, and provide forensic analysis tools to

research identified threats and search for suspicious activities.

Also see Managed Detection and Response (MDR).

Exchange, Exchange Online or Hosted Exchange:

A Microsoft software product or online service used for business email processing. In addition to sending and receiving email, Exchange also allows you to share calendars and tasks with other team members. When initially released, it was one of the first mail servers that enabled you to sync your mailbox, contacts and calendar to all of your devices.

Email Archiving:

Archiving, when speaking of email, is a service that catalogues and securely keeps a copy of every email sent and received by anyone at your company, even if they permanently delete the message from their mailbox. Made famous by the Hillary Clinton lost email scandal, email archiving is something several industries and businesses are now required to implement. Email archiving is either priced per user per month

(recommended) or based on storage used for all archived emails.

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 an external drive or an offsite backup provider on a regular schedule. While this is a great choice for certain situations, BCDR image-based backup is superior and will make the recovery process go much faster than a file and folder backup.

Firewall:

A firewall is a network security appliance that monitors and controls incoming and outgoing network traffic to establish a barrier between a trusted network (like your business) and an untrusted network, such as the Internet.

Hacker:

"Hacker" is a term now used for a person who tries to gain unauthorized access to a network or computer systems with malicious intent.

Interestingly, in the early days of computers, "hacker" was a complimentary term used to refer to a programmer who pushed the functional boundaries of hardware & software. Kevin Mitnick, one of the most famous cyber criminals of all time, explained that "hackers" created the first algorithm to accurately model water flow back in the 1970's.

However, just as early programmers pushed technological boundaries, modern cyber criminals also must push the boundaries of technology in order to gain unauthorized access to systems. So, the meaning of the term evolved to become synonymous with cyber criminals.

Hosting:

Hosting describes the function of computer or server that runs a specific application. The host computer is accessed over the network and/or Internet. A host may offer resources, services, or

applications to employees, clients and/or third-party vendors.

Infrastructure as a Service (IaaS):

Infrastructure as a service (IaaS) is a type of cloud service that offers essential processing, storage and networking resources to businesses on-demand, on a pay-as-you-go basis. Migrating your organization's infrastructure to an IaaS solution helps you reduce maintenance of on-premises equipment, save money on hardware and gain enhanced reliability and up-time. IaaS solutions give you the flexibility to scale your IT resources up and down as needed. They also help you quickly set up new applications and increase the reliability of your most critical IT infrastructure.

Information Security:

Information security is managing risks to the confidentiality, integrity, and availability of information using administrative, physical, and technical controls.

IP Address:

An IP address is the unique identifier for a computer or device on a network, like the street address for a physical building. There are two different types of IP addresses: public and private. Private IP addresses are assigned to devices inside your network, such as computers and printers. Public IP addresses are assigned to devices accessible on the Internet (such as your firewall). Your internal computers, with private IPs, all share one public IP address assigned to your firewall.

Malware:

Malware is a shorthand term referring to malicious software. Malware is defined as any software that is used to interrupt or disrupt operations, gather sensitive information, or gain unauthorized access to files or programs.

Managed Detection and Response (MDR):

Expands on the concept of EDR to view the network as a whole. Yes, the network is comprised of

individual devices, but a threat distributed across many of those devices may not trigger any action. Monitoring the aggregate network traffic can reveal otherwise undetectable threats.

Microsoft 365:

Formerly called “Office 365”, Microsoft offers their Office suite of applications (Word, Excel, PowerPoint, Access, Outlook, Publisher, OneNote) as well as Microsoft Exchange email services for a monthly fee. Subscribers never have to purchase any of these applications, and they are allowed to both install them on their computer or phone and use them through a web browser. For most businesses, a Microsoft 365 subscription ranges between $25 and $90 per month per user, and each staff member is required to have their own subscription.

Microsoft Azure:

Azure is Microsoft’s public cloud platform and is offered as an alternate to having servers and infrastructure on site in your office. It provides various

cloud services, including servers, storage, networking, and backup and disaster recovery. Businesses can pick and choose from these services to develop and scale their infrastructure.

Network:

The term “network” refers to two or more devices (computers, phones, tablets, etc.) that are connected to one another for the purpose of communicating data electronically. The computers and servers in your office, the connected electronic devices in your home, and the Internet are three examples of a network.

Network Switch:

A network switch (or just “switch”) is the device that allows network devices to connect to each other. Typically, the cable from each computer wall jack runs through the wall to a patch panel. At the patch panel, a patch cable connects it to the switch. The network switch is a key factor in determining the speed of the network.

Patch Panel:

A piece of network equipment typically in a server or utility closet, a patch panel provides an organized way to connect all the network cabling installed in the walls of a building/office. Typically, each port on a patch panel is numbered. For cable management and to simplify troubleshooting of connectivity issues, it's common to label the wall plate in each office with the corresponding patch panel port number. For example, a network jack in an office labeled "3" will connect to port 3 of the patch panel. A patch cable will then connect port 3 of the patch panel to the network switch.

Phishing

Phishing is the practice of sending fraudulent emails appearing to be from reputable individuals or companies in an attempt to induce individuals to reveal personal information such as passwords and credit card numbers. Phishing is one of the most simple and common techniques used by criminals to wreak havoc on a company's network. Phishing is 100% preventable with employee training. It can also

be mitigated with anti-phishing and anti-spam solutions.

Power over Ethernet (PoE):

Power over Ethernet is a technology that delivers low-voltage power over the same network cable used to communicate with devices like wireless access points, VoIP telephones or IP cameras.

Often these devices are not located near a power source. Rather than incurring the cost to have an electrician install power outlets at those locations, it's much easier to run a single network cable to the device for both power and communication.

A PoE injector is used to add power to a network cable. Some network switches have PoE capability built-in so that separate injectors are not needed.

Ransomware:

Ransomware is a type of malicious software that infects a computer and restricts users' access to data until a ransom is paid to unlock it. Ransomware variants have been observed for several years and

attempt to extort money from victims by displaying an on-screen alert. In recent years, ransomware has resulted in companies both large and small paying fines from thousands of dollars to over $70 million.

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 person using the computer. When this is happening, the user often doesn't even know that work is being done.

RMM software is one of the tools that alerts 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, 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 to increase availability if something goes wrong. For example, servers often store the same information on multiple hard drives so that if one fails, data isn't lost. Redundant power supplies are also common on servers.

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 evolved. If a small organization needs a server, it's likely more affordable than you think.

Spam/Spam Filtering:

Junk or unsolicited email is known as spam. Once your email address begins receiving junk mail, it's very hard to stop without changing your email address.

Spam filtering is a service that examines email before it gets delivered in an attempt to judge whether the message is legitimate or not. If it's believed to be junk, it isn't delivered. Instead, it's kept in quarantine or separate folder from your inbox. Many email services, such as Google Workspace and Microsoft Exchange Online, provide basic spam filtering. However, if you continue to receive junk mail that isn't being caught, an "advanced" spam filter can provide more exhaustive junk mail filtering.

HINT: To reduce the amount of spam going to your business email account, avoid using your primary work email when you need to create accounts on websites to simply obtain information. Instead, use a free @gmail.com or @outlook.com address.

Software as a Service (SaaS):

In its most basic form, SaaS is a pay-as-you-go model for software. Companies provide software and support on a subscription basis instead of a large one-time purchase followed by annual support and upgrade costs. Microsoft 365 and QuickBooks subscriptions are examples of SaaS applications.

Uniform Resource Locator (URL):

A URL is the global address of documents, websites and other resources on the web.

As an example, google.com is the domain but https://www.google.com is the URL for Google's search page.

Voice over Internet Protocol (VoIP):

VoIP is a category of hardware and software that allows you to use the Internet to make phone calls and send faxes instead of using an analogue 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 phone system-related expenses. Often, VoIP phone services allow you to log into an easy-to-use website to change the behaviour 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.

Virtual Private Network (VPN):

A VPN a is a method of using public infrastructure (the Internet) to connect private resources (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 servers and computers between remote offices, from home or while traveling. Your firewall or a cloud service typically manages VPN connectivity.

Web Hosting:

Often referred to simply as “hosting”, web hosting is the service of providing servers and other required equipment to both store and run a website. Every single website we access over the Internet is hosted somewhere in the world. The term “hosted” refers to the provider and physical equipment responsible for running that specific website we are viewing.

(Wireless) Access Point (WAP or AP):

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.

Unfortunately, the complexity of technology makes it easy for a business owner to fall victim to an incompetent IT firm. 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 IT firm, but also, 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 our clients. I want to help business owners

see the true competitive advantages technology can deliver to their business and not just view it as an expensive necessity and source of problems.

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

Scott Birmingham, C.E.T., C.I.M.
Birmingham Consulting Inc.
21 Mill St. N.
Waterdown, ON L0R 2H0
289-895-8948
publishing@birmingham.ca
www.birmingham.ca

Do any of these questions sound familiar?

Do you wonder if IT really understands the business risks posed by cyber security?

Are you upset with IT who seem much more interested in gadgets than in security?

Confused about the difference between IT, Security, and Compliance?

Are you unsure of what critical questions to ask when choosing an IT service provider?

Confused about what should/shouldn't be included in an IT support contract?

Are you upset with IT/security invoices that don't make any sense?

Are you fed up with being locked into a long-term support contract?

If you answered 'yes' to any of these questions,
this book is for you!

ABOUT THE AUTHOR:
Scott Birmingham has over 30 years technology sector experience in engineering, management, IT, and cyber security. Because of Scott's engineering roots, Birmingham Consulting brings a practical perspective to the information security industry, and his team shares a common goal: ***Resilience.*** Practically speaking, there's no such thing as perfect security; so Birmingham focuses both on protecting businesses ***and*** preparing them to respond when protection isn't enough.

BIRMINGHAM
CONSULTING

21 Mill Street North, Waterdown, ON L0R 2H0
www.birmingham.ca

7 10497 34799 0