THE COMPLETE GUIDE TO

Outsourced IT

COM · PRO

Managed Business Solutions

ABOUT THE AUTHOR:

The Complete Guide to Outsourced IT

Hey, I'm Mike. Here's my super professional third-person bio:

Mike Hamfelt is a Partner and Vice President at Com Pro. He's been with Com Pro since 2015, and is passionate about process improvement, strategic planning, creating engaged cultures and helping organizations grow.

Add Mike on LinkedIn! He'd be happy to chat with you regarding just about anything to do with business including how Managed IT can help your business perform.

Find Mike On

LINKEDIN AT:
linkedin.com/in/mike-hamfelt-cpa-cma-81a52224/

ABOUT:

About Com Pro Managed Business Solutions

Since 1998, Com Pro has been committed to helping businesses improve office productivity and IT infrastructure through expert technical support, best-in-class office equipment, and caring customer service. Leave your IT services to us and get focused back on what you do best.

Take a look at our Managed IT Services.

LEARN MORE

We're proudly based in beautiful British Columbia, just like many of our awesome clients. We support a wide variety of industries, such as law, financial services, real estate, architecture, engineering, education, healthcare, government, manufacturing, automotive, non-profit, and more. Don't see your industry here? We'd still love to talk.

CONTACT US

EMAIL AT
admin@comprobusiness.com

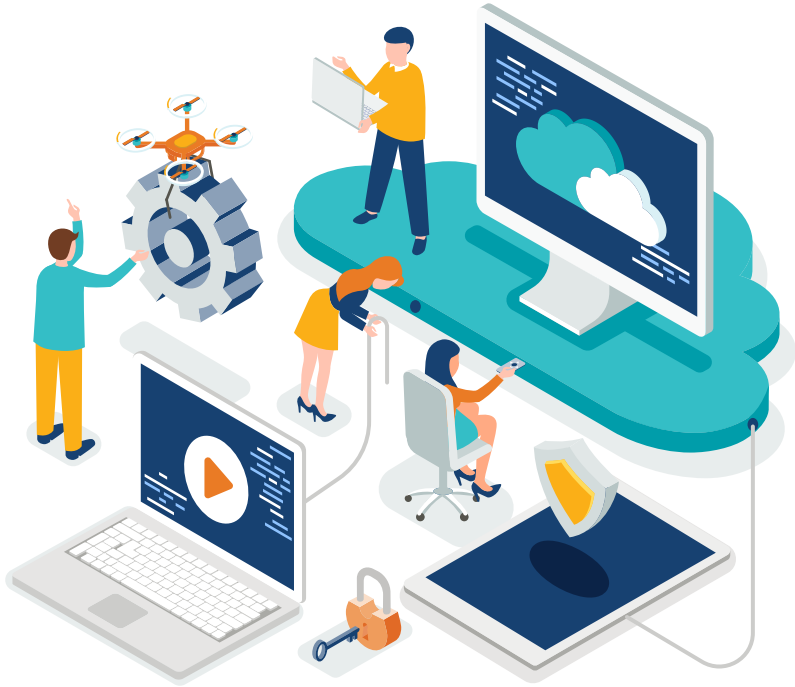
ON LINKEDIN AT
company/com-pro-business-solutions-ltd

ON FACEBOOK AT
@comprobusiness

ON INSTAGRAM AT
@comprobusiness

TABLE OF CONTENTS:

What Is Outsourced IT?



OUTSOURCED IT SERVICES IS WHEN YOU HIRE AN EXTERNAL COMPANY TO MANAGE ALL OF YOUR IT BUSINESS PROCESSES.

In short, outsourcing your IT services is when you pay someone else to handle the least favourite part of your business, so you can focus on what you're great at. These companies, often called managed service providers (MSPs), specialize in remotely managing and anticipating the needs of their customer's IT infrastructure.

MSPs are a technology resource for businesses that have limited IT support, or for those who don't have a full IT team in-house. They can manage all of your business' IT, or they can assist your team in specific areas, such as cybersecurity, where they monitor and neutralize threats to your network. If you're in a high growth period or simply know your tech stack could be better, an MSP can suggest improvements to your IT infrastructure, such as cloud solutions or new hardware that enhances productivity. They can also mitigate and minimize risk by helping you with disaster recovery plans.

Outsourced IT is more than simply calling a technician to fix a server problem or broken computer. It's about finding a trusted managed service provider (MSP), to protect your digital infrastructure and your data, so you can focus on building your business.

Why Should I Outsource My IT Services?

Many businesses choose to partner with a managed service provider to handle their IT requirements because it's a cost-effective, hassle-free way to manage IT. While you may be technically proficient, or even have an in-house IT technician who's a computer wizard, as your company grows it could become more difficult to handle all your IT needs in-house. More importantly, it could become dangerous when you're holding your customers' sensitive data on cloud platforms.

1. **TO SAVE MONEY.** Rather than hiring and training full or part-time IT staff to manage and support certain aspects of your business, it's usually more cost-effective to select a service provider who is an expert in that field... and has the staff to manage it. Hiring an in-house IT support manager can increase downtime and reduce efficiency.

   Internal employees can get burnt out, take sick leave, or leave the company altogether. An MSP is always there and can assign a dedicated team of IT professionals who have the skills needed to solve issues quickly. It also costs more to hire, train, and retain your own full-time IT staff.

2. **TO MAKE BUDGETING EASIER.** Outsourcing IT creates cost savings. Unlike the billable hours of an in-house employee, which are highly variable and often unpredictable, an MSP will often have a defined monthly fee or flat up-front cost that covers all the necessary personnel and resources required to do the job. This makes it a predictable monthly expense for which you can easily budget and keeps your accounting team happy.

59%
Of Businesses
use outsourcing as a cost-cutting tool

57%
Of Businesses
outsource because it allows them to focus on their core business

3. **TO REDUCE CRITICAL RISK.** You risk critical downtime if your in-house IT manager is off the clock, or worse, if they call in sick or quit unexpectedly. MSPs will provide as-needed, round-the-clock IT support for emergencies, whether that's a massive security breach, or you accidentally saved your presentation for tomorrow somewhere... you just forget where, exactly. Additionally, their expertise, and industry-specific knowledge, will introduce you to new ways of lowering risk in the areas in which they serve.

4. **TO PROTECT DATA.** Whether you're in processional services and handling the private data of your clients, or you're a sales organization with thousands of customer credit cards on file, your data is important. And so is your reputation. Let a team of experts assume responsibility for providing critical infrastructure to keep you and your clients safe.

5. **TO IMPROVE BUSINESS OPERATIONS.** Outsourcing your IT services can improve overall business operations. Yes, really! You're inviting a third-party expert to review your existing processes and provide valuable insights. With fresh eyes, they can spot inefficiencies, tailor improvements for your unique industry or needs, and help to streamline your overall digital services.

6. **TO HAVE ACCESS TO FULL SERVICE, 24/7 SUPPORT.** Because an MSP manages their own staffing, you won't have to worry about trying to train a new IT manager to understand your existing systems. Plus, you'll have access to someone who understands your IT and business needs when you need them. That feels a whole lot nicer than needing to phone your employee from IT at midnight and hope he's still awake because your server broke down again.

7. **TO LEAVE IN-HOUSE IT TO MANAGE STRATEGIC PROJECTS.** We know what you're thinking—you love your employees from IT! That's fine, you can keep them! We promise you; they'll love outsourced IT as well. Having a managed service provider means your existing IT team can focus on big picture strategic tech improvements, while your outsourced team can handle the monotonous daily activities and emergency support.

Mythbusters: The 10 Most Popular Myths About Cybersecurity

MYTH 1

Most Security Threats Come From Outside The Organization

FACT:

Many security threats come from within an organization. They're accidental, but that doesn't make them any less scary. 46% of employees admit they transfer files between work and personal computers, and 13% admit to using their personal emails when they can't connect to an office network.

MYTH 2

Passwords Offer The Best Security

FACT:

While passwords offer some protection, they are still not people-proof. 70% of small and mid-sized businesses reported lost or stolen employee passwords.

MYTH 3

Our Antivirus Software Will Protect Me From Online Threats

FACT:

Information hacking is often hidden in something that looks innocent. Many phishing programs disguise themselves as emails or unsolicited attachments, and 57% of companies have experienced phishing attacks that attempt to steal sensitive or personal data.

MYTH 4

Cyber Threats Are Overexaggerated

FACT:

On average, a hacker attack occurs every 39 seconds. That's 2,244 attacks every single day.

MYTH 5
Our Business Is Too Small For Any Real Attacks

FACT:
Almost half (43%) of cyberattacks target small businesses and Canada has been identified as the second largest market for cyber-attacks, costing Canadian small businesses almost $2.3 billion dollars in ransom demands last year. Yes, that's billion with a b.

MYTH 6
Our Office IT Has Security Features Already Built In

FACT:
Many businesses have security features that go unused. 23% of small and mid-sized businesses don't use endpoint security protections like encryption tools or firewalls, which means their devices are vulnerable to harmful programs.

MYTH 7
Hackers Can't Really Affect Our Business That Much

FACT:
1 in 5 small businesses have been forced to close due to high ransomware demands. On average, cyberattacks cost a business $200,000 to resolve, and many never recover from the revenue loss or the loss of consumer trust.

MYTH 8
If Our IT Systems Are Seriously Breached, We Will Detect It Right Away

FACT:
IT monitoring can protect you, but if your credentials have been compromised, a hacker could have access to bypass perimeter security. The average detection time for a breach is currently 206 days.

MYTH 9 Viruses Are The Main Threat To Business Security

FACT:

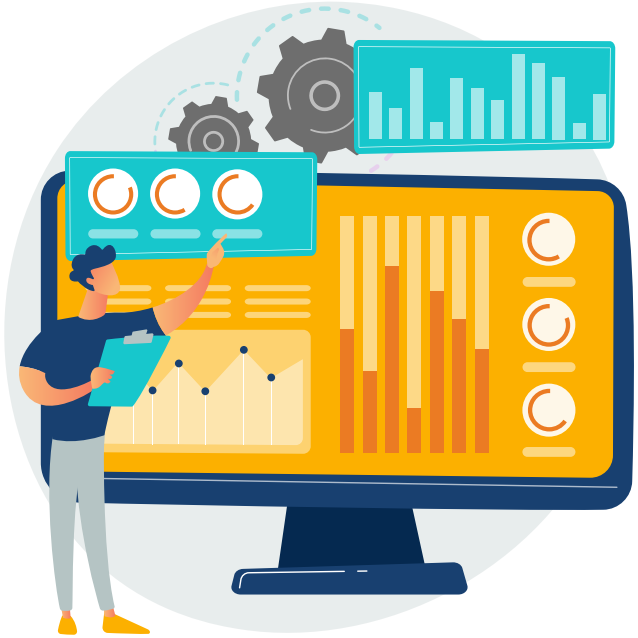
Ransomware is becoming an increasing problem, with ransom demands skyrocketing into millions of dollars. In fact, 85% of managed service providers identify ransomware as the main malware threat to small and mid-sized businesses.

MYTH 10 Security Breaches Only Affect My Business Operations

FACT:

In the first half of 2019, 4.1 billion records were exposed by data breaches, some of which did irreparable damage to a brand. 65% of customers affected by a breach lost trust in that organization, with one in four taking their business elsewhere.

How Do I Know When It's Time To Outsource My IT?



We like to say that if you're wondering if it's time to begin outsourcing some (or all) of your IT functions... then it's probably time. But the final decision will always be a personal one that depends on numerous factors.

Your decision to finally outsource can be for many reasons, including what phase of growth your company is in, whether customer data security is top of mind in your industry, or whether you have work-at-home staff that require more robust IT security and infrastructure.

IF YOU'VE CAUGHT ANYONE IN YOUR BUSINESS SAYING ANY OF THE FOLLOWING, IT'S *DEFINITELY* TIME TO OUTSOURCE:

"I'm suffering too much downtime due to outages, lack of support or maintenance issues."

"Our overall company performance has been affected by a lack of service and support."

"We overspent again on our IT budget! I can never guess how much everything will cost."

"My company has suffered data losses because of our inability to come up with a solution."

"Handling a workforce that works partially from the office and partially from home has us totally overwhelmed."

If you relate to the above statements, it likely means you could *benefit* from outsourcing some of your managed services. Hire an expert and experienced MSP like Com Pro and you'll rest easier knowing that you have a reliable, *dependable* provider managing your IT.

Which Of My IT Tasks Should I Outsource?

As your business grows and evolves, you will inevitably come to that fork in the road where you need to decide what IT Services should be kept inhouse and what can be outsourced. Maybe you know you're ready to just outsource the whole thing and enjoy a hassle-free experience. But if you're a growing small business, outsourcing absolutely everything might be too costly for right now. Here are the top tasks that other businesses are outsourcing.

ACCORDING TO STATISTA:

51%
OUTSOURCED
Software Maintenance

32%
OUTSOURCED
IT Infrastructure & Help Desk

29%
OUTSOURCED TO
Monitor & Manage Networks

12%
OUTSOURCED THE
Entire IT Department

- **REPETITIVE TASKS THAT CAN'T BE AUTOMATED –** Don't waste your company's time, money, and talent on repetitive tasks. If a job can't be automated, it can usually be outsourced. Things like routine IT maintenance, time-consuming tasks like system updates and backups that are critical to performance, or any day-to-day IT needs can be delegated to an MSP, so your in-house IT managers can focus on the big picture.

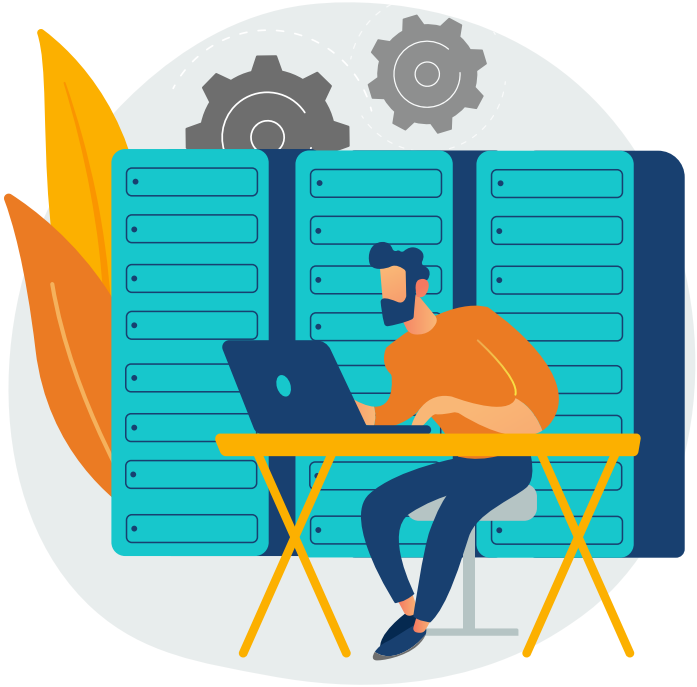
- **HARDWARE MAINTENANCE –** One of the best decisions you can make is to *outsource* your hardware maintenance. Who has time to go around sourcing, updating, and replacing all outdated or inefficient hardware? An MSP can troubleshoot any hardware issues, take care of routine maintenance tasks, and use their expertise to guide you toward better investments in technology, all for a reduced, flat monthly fee.

- **IT ASSESSMENTS & IMPROVEMENTS –** It's often best to gain some outside perspective, especially when it comes to assessing your IT infrastructure, security requirements, and plans to scale up. This is where an external assessment can be helpful. Outside observers can quickly uncover inefficiencies, gaps, and areas for improvement. Having an outside perspective can help you build a more robust IT infrastructure that can give your company a competitive edge in your respective industry.

- **CLOUD SOLUTIONS & COMPUTING –** Over 95% of companies use cloud computing in some form or another, with small businesses running over 80% of their workloads on the cloud. Hosting your own cloud-based system can be expensive and time-consuming. By outsourcing your cloud computing you can still digitize your operations to remain competitive, while delegating the responsibility for backups, updates, and security to a team of IT experts.

- **SYSTEM SECURITY –** With the increase in work-from-home arrangements, cloud solutions and storage, and more business functions going online, cybercrime has continued to rise. Over the last two decades, data breaches have increased almost tenfold and the average cost to manage a business' breach was $9 million USD! It can take a lot of effort and resources to keep ahead of cyber threats. Select an MSP that provides 24/7 monitoring to make your data security their full-time job.

The "New Normal": Protecting Remote Workers



The Covid-19 pandemic has forever altered the way we do business. With many employees being forced to work from home, organizations had to adjust to the new normal of remote work, basically overnight. Few people were more panicked than IT leaders, who suddenly had to attempt to maintain cybersecurity with employees working from home or personal devices. Some businesses were already set up to manage at least some remote work, but many others were forced to scramble to set up all new remote support and security operations, without time to prepare for this change.

As we begin to go back into the workplace, many employees are requesting that work-from-home options continue. How will you prepare for both in-office IT support, and remote work support? How will you keep your business safe?

When it comes to IT security, it takes a team effort. Employees have the responsibility of keeping their systems secure while working from home, and you bear the responsibility of educating them on what to do and what to avoid. A Managed Service Provider can help your organization create security guidelines that your employees can then implement to work as securely as possible.

IN THE MEANTIME, HERE ARE SOME CRUCIAL IT SAFETY TIPS YOU CAN SHARE WITH YOUR TELECOMMUTING STAFF RIGHT NOW.

DON'T SCOLD, BUT UPHOLD SECURITY GUIDELINES.

The worst thing you can do is lecture your employees. You can expect them to take necessary precautions when working from home, but you might be surprised by how many people simply don't understand how to keep themselves and their employer safe.

Educate your team on the subtle threats that lurk, such as unsecure smartphones, public Wi-Fi, and phishing schemes. Scolding employees can create shame and fear, which prevents them from reaching out to ask for help if something does go wrong.

STAY SAFE WITH THE RIGHT SOFTWARE.

Firewalls, virus checkers and antivirus software offer good protection, but only if they're turned on. Many people opt to bypass these safety measures because they might restrict attachments and files, or stop you from visiting certain websites.

Make sure your employees download all required IT security software and encourage them to run software updates as soon as they're available. Send routine email reminders if need be.

LOCK UP BEFORE YOU LEAVE.

You wouldn't leave your new car parked outside without locking it up. Home computers and workspaces are no different. Security threats can lurk anywhere, especially when you share your home or workspace with others.

Anytime you step away from your computer, laptop, or phone, make sure to lock your devices with passwords. If your employees have access to particularly sensitive data (such as a law firm, or accounting firm), advise staff to set up their workspace in a separate room if possible. A room that can be physically locked provides an extra layer of security.

KEEP PERSONAL AND PROFESSIONAL DEVICES SEPARATE.

Whether you're working from home, the office, or both, it's important to keep your devices separate. Many of us think nothing of sending a work email using a personal smartphone or email account. But this means you might be sending company info using less secure devices that can easily be hacked.

For sharing company files, always use your work email and devices, never personal ones. Create different, complex passwords for each system or software login. Never use the same passwords for both personal and professional accounts. For more security, a VPN (virtual private network) can give your team access to a private network that encrypts data transfers and hides user locations and IP addresses.

BACK UP BUSINESS DATA SAFELY

Data storage is equally as important. External hard drives and USB sticks are convenient, but they can be easily misplaced, stolen, or broken. In this digital world, computer files are often one of the most valuable assets of your company. Today's cyber criminals are savvy. Information is now their target. Back up your work data to a secure, company-approved cloud storage system.

Cloud storage not only enables employees to access their work from both home and the office, but they also enable your IT team to monitor, encrypt, and clean data.

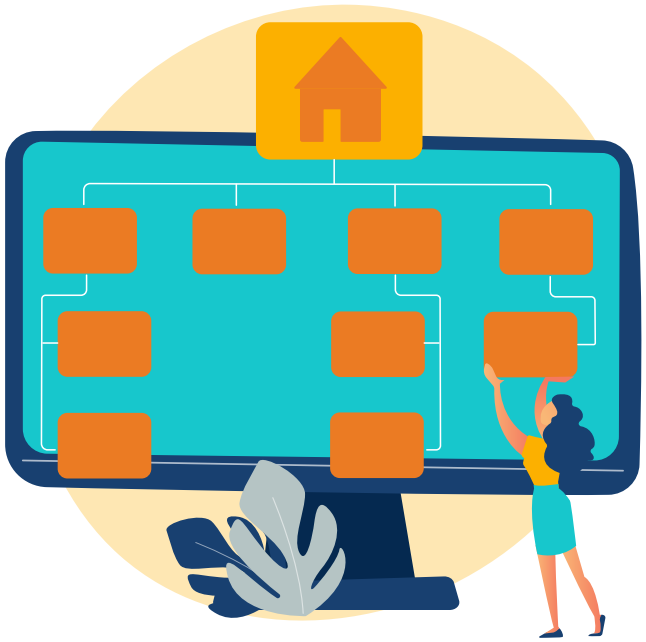
PLAN FOR THE WORST

A security breach can happen, even with the best remote work practices and highest security precautions. Always have an alternate plan for when things go sideways so your business experiences minimal disruptions and downtime.

A contingency plan will keep everyone feeling calmer, even in the worst-case scenario. If you don't already have a business continuity and disaster recovery plan, now is the time to start one. An IT provider can help you design a plan with actionable steps for dealing with security issues, should they arise.

OUTSOURCE IT TO MANAGE EMERGENCIES

If a data breach does happen, you'll want to have all hands on-deck. Outsourced IT can provide your organization with a 24/7 support desk to assist with potential threats, as well as assisting employees that are working remotely after hours.



The 4 Tools You Should Already Be Using To Protect Your Business

But if you aren't? No worries. An MSP can help you get these 4 tools in place quickly and securely.

1. SECURE VPN TECHNOLOGY

Many employees admit to leaving a work device unattended in public while working remotely, or to using public Wi-Fi to send and receive work files. It's all too tempting to answer that work or customer email on your personal smartphone at the kitchen table or in line at the coffee shop. But that also means that others could be using that shared network to spy on your activities or to gain access to your company's IT systems.

As the name suggests, a virtual private network (VPN), allows your team to access a private, secure network, even if they use their own household or public Wi-Fi. A VPN can mask a users' location and IP address and encrypts data as it moves back and forth across the internet. It doesn't mean your activities cannot be monitored while using a VPN. Website cookies can still track your online "movements". But a VPN offers another layer of protection that can stop others from accessing your sensitive company data.

2. MULTI-FACTOR AUTHENTICATION

Another risk that is often posed by remote working is unauthorized logins to company systems. When employees work in an office, you control the environment and the level of security. When your employees work from home, you face potential risks.

Multi-factor authentication can protect your business by requiring users to provide two or more pieces of evidence to access devices and systems. This is usually something only the user knows, such as a key code or PIN, or something only an authorized user would have in their possession, such as a badge or smartphone. You can even go a step further and use things like fingerprint or voice recognition. By implementing this extra step, you can reduce the risk of unauthorized access.

3. ACCESS CONTROL

It's also important to control the level of access for each remote worker. Not everyone needs to access every single IT system. Good access control means you know who should access your company data (authorization), and you have the means to ensure the right person is granted access (authentication). In other words, you have gatekeepers, like multi-factor authentication, in place that ensure that the right person accesses the right systems.

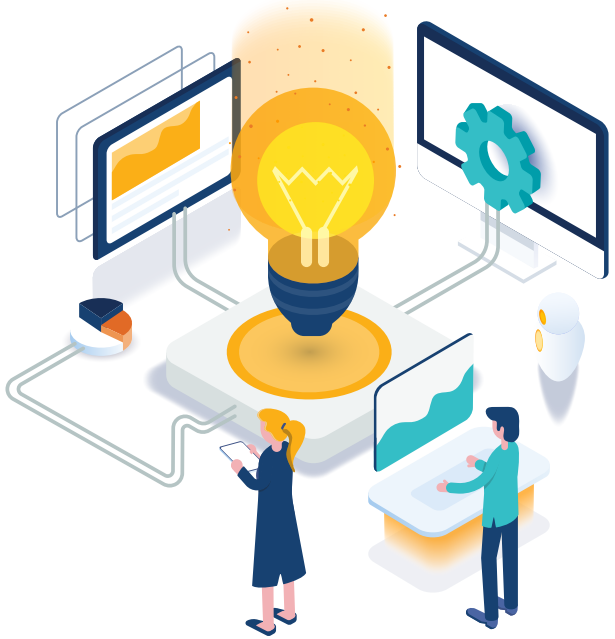
Every business needs some form of access control, especially if employees work from home and require access to company resources and networks. By limiting access to only the systems and data a worker needs to do their job, you lessen the risk of info leaks and security breaches.

4. SECURITY TRAINING

All the above tools can keep your business safe. However, they don't account for human error or negligence, so a vital piece of the puzzle must involve security training for remote staff. Security training can help employees to comprehend the IT risks involved in working from home. And by outlining and documenting your security policy and best practices, you can give remote staff the education they need to keep themselves and the company safe.

Distribute a clearly *written* security policy to all remote workers. Outline how to spot threats, how to report a problem, and steps employees can take to reduce security risks. Remember, not everyone speaks "IT", so make sure it is easy to follow and make sure your team understands their responsibilities. An outsourced IT provider may already have versions of policies that they can help you implement, without needing to start from scratch.

What Should I Look For In An Outsourced IT Provider?



A reliable and knowledgeable MSP should be concerned with keeping your IT operations secure and efficient. They should be responsive, agile, innovative, and cost-effective. Most importantly, they should be there for your organization and your employees, when and where you need them, even if that falls outside of business hours. There's nothing worse than having projects on hold while you wrestle with an IT issue.

HERE ARE THE 6 MOST IMPORTANT THINGS TO CONSIDER WHEN SELECTING YOUR OUTSOURCED IT PROVIDER:

1. **FAST RESPONSE TIMES.** When a tech emergency arises, the last thing you want to experience is a busy signal from your IT provider. Before committing to a provider, ask them about their emergency response services. At Com Pro, our 24/7 remote monitoring for emergencies and an industry-leading response time rate of 2.8 hours, alleviates stress and keeps our customers safe and calm during emergencies and urgent requests.

2. **FLEXIBLE, CUSTOMIZABLE SOLUTIONS.** Select a provider that will ensure you have all the services you need, but aren't paying more than you have to. Solutions that are tailored to your business needs and industry will ensure your IT is built to suit you, not the other way around.

3. **BUNDLED AND PACKAGE OPTIONS.** Take the hassle out of budgeting by selecting a provider that has monthly or annual packages. Sure, a-la-carte can seem appealing at times, but a full-service plan will cover any and all issues that potentially arise, all within one simple bill. Don't get caught trying to slip a massive IT bill past your CFO if you experience an unexpected security breach. Your accounting team (and your purse strings) will thank you for a reliable monthly expense.

AT COM PRO, WE CAN ALSO BUNDLE ADDITIONAL OFFICE SERVICES, SUCH AS MANAGED PRINT.

4. **LOCATION, LOCATION, LOCATION.** In today's cloud-based world, most IT concerns can and should be managed remotely. But there are still some tech support issues where you'll be grateful to have a friendly face show up at your office to save the day. At Com Pro, we live and work in BC. Should you partner with us and need onsite support, we'll be there—fast, friendly, and ready to fix it.

5. **SUSTAINABLE PROVIDERS UPHOLD YOUR GLOBAL SUSTAINABILITY VALUES.** Being more environmentally conscious has been top of mind for businesses across all industries in recent years. If this is an important value to your organization, you'll want to partner with an MSP who shares those beliefs and participates in sustainability programs. At Com Pro, we believe in keeping our services as environmentally conscious as possible by refurbishing print and office equipment to reduce landfill waste, sourcing energy efficient equipment, and partnering with organizations that are committed to sustainability. For example, we donate a portion of print proceeds to reforestation projects around the world in partnership with PrintReleaf.

6. **SOLID REPUTATION.** It goes without saying that before you do business with any company, you should be checking their references. With something as critical as cybersecurity, you can't afford to make mistakes. At Com Pro, we've been in the business since 1998. Yep, that's right, that's back when dial up was still a thing. We've been there, done that. It's our commitment to share our knowledge with our customers, and ensure their IT is taken care of quickly, safely, and securely.

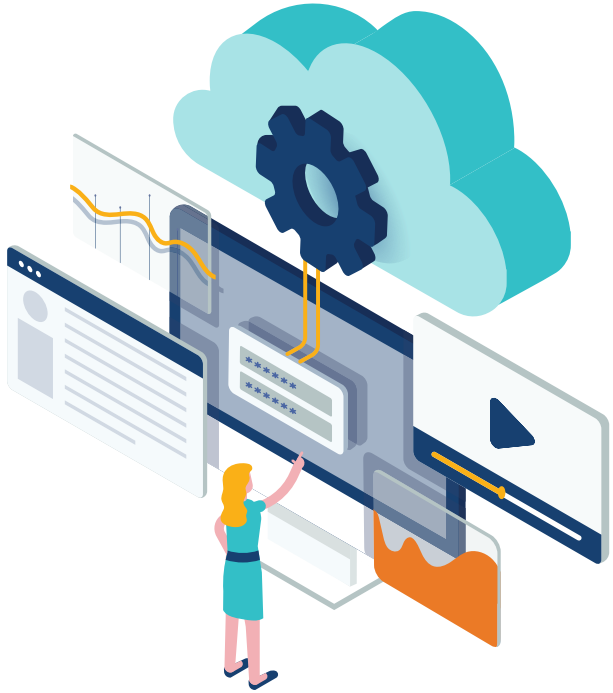
WRAPPING UP:

When you delegate your IT management to an external partner, you will find that you're able to refocus your energy on other tasks within your organization, thereby freeing up your internal staff so they can devote their time to projects that advance your business.

Finding a trusted MSP isn't always easy. You should look for Managed IT providers like Com Pro, who have a reputation for reliability and excellent customer service.

THEY SHOULD OFFER:

- Flexible, customized solutions
- Help desks that are locally-based and offer support beyond normal working hours
- Service costs that are reasonable, and fixed monthly rates for easy budgeting
- The latest IT monitoring software and security options
- A skilled team of IT professionals who can help advise you on the best IT solutions and investments, with experience in business continuity, and disaster recovery plans.

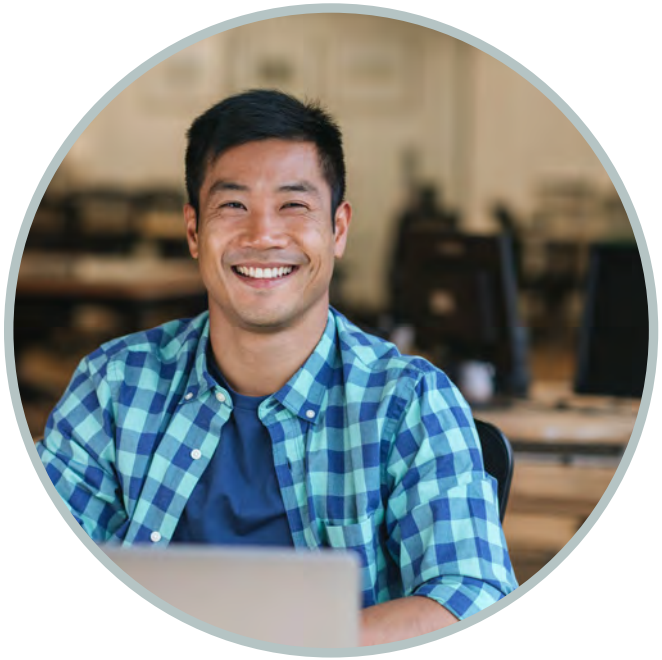


The best vendors will seek to secure a favorable deal for your company. They shouldn't try to "up sell" you with features you don't require. Instead, they should focus on selling you equipment that matches your requirements at a *reasonable* price.

Lastly, check out customer reviews and case studies. Past and present customer feedback can give you great insight into which companies actually *value* their customers. Reputable companies like Com Pro have a solid reputation among local businesses. It's also a good sign if they offer Managed IT Services alongside Managed Print, because their experts can work together to ensure that all your office infrastructure, security and remote work needs are also met.

GET IT SOLUTIONS THAT HELP YOUR COMPANY COMPETE IN THE MARKETPLACE.
COM PRO CAN TAKE CARE OF ALL YOUR IT, SO YOU DON'T HAVE TO.
CALL US AT 604-574-8623 OR VISIT OUR CONTACT PAGE.

See What Our Customers Are Saying...



"Our experience has been spectacular so far. Com Pro has made every effort to accommodate our budget and get our business set up for success. You can truly tell that everyone at this company cares about their customers."

— Rachel Charles, West Coast Windows

"Fair, honest pricing, and good quality service. Knowledgeable group of employees who took time to explain some of the more complex IT issues we had so that I felt comfortable making an informed decision. Treated me right. Highly recommended."

— Scott Grover, Mueller/Singer Valve

"Every time we have a problem, it is promptly addressed. The technicians are efficient and take time to explain the problem, what's being done to fix it and how we can prevent this from happening in the future. They are never rude or impatient with questions or explanations. I appreciate the service we receive from Com Pro very much!"

— S. Aragones, Trinity Western University

"We've always received quick and friendly service from Com Pro. They will pop in from time to time just see if we are good. When we have a service call, they always come fast and fix the problem right away."

—Shari R., Administration, Johnston Meier Insurance Agencies Group

COM · PRO
Managed Business Solutions

CONTACT US

Head Office:
18515 53rd Avenue
Suite 110
Surrey, BC, V3S 7A4

TF: 1-866-266-7761
T: 604-574-8623
F: 604-574-8634

Vancouver Office:
1108 W 8th Avenue
Vancouver, BC, V6H 3Z5

T: 604-664-8901
F: 604-900-3377
E: admin@comprobusiness.com

CONTACT US