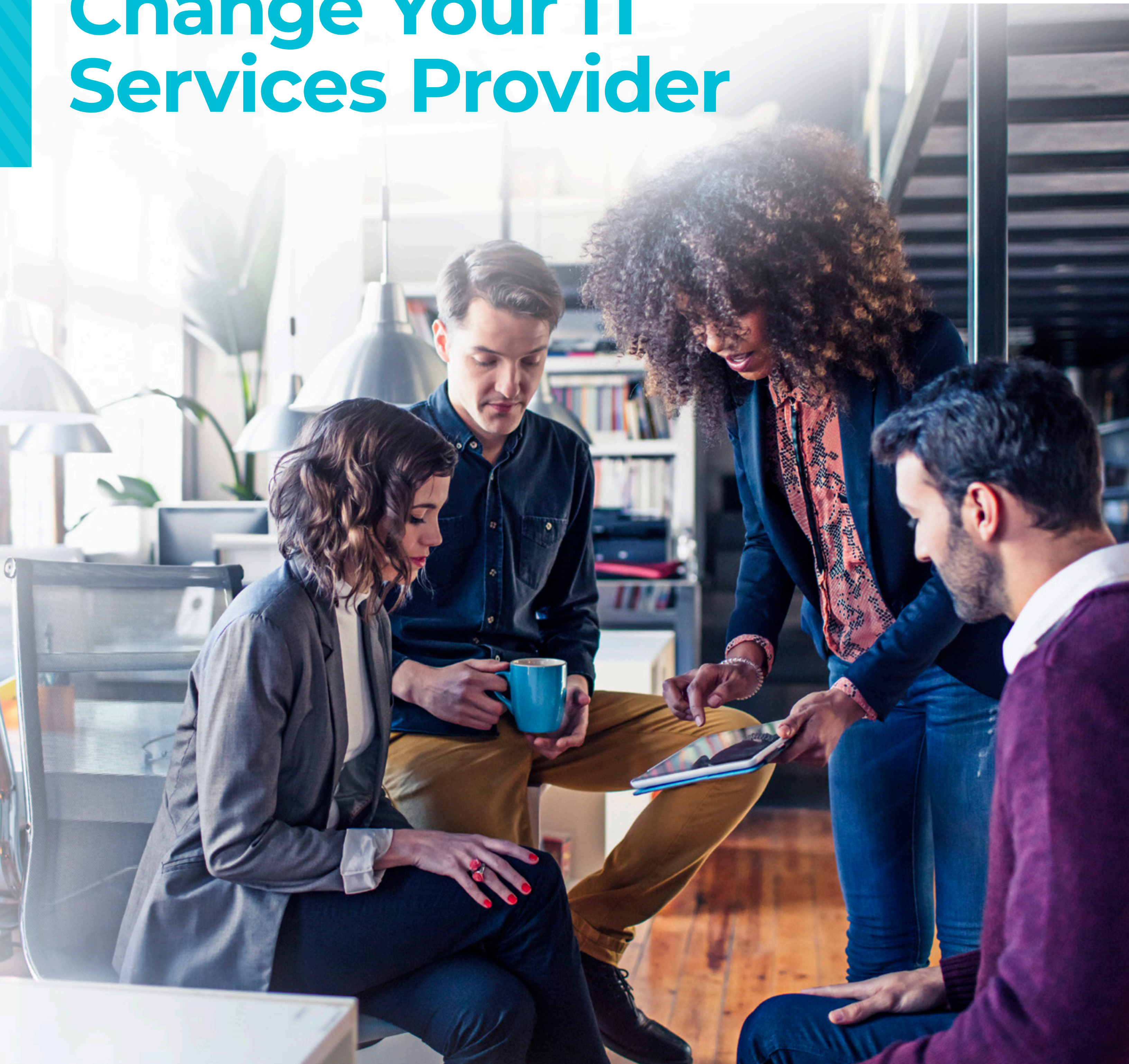
CompuCom® | MANAGED IT as a SERVICE

6 Signs It's Time to **Change Your IT Services Provider**



Choosing the best managed IT services provider (MSP) for your company requires you to have a thorough understanding of your technology needs, both today and in the future. The company you originally chose to handle your IT services – while it may have been suitable when you first selected it – may not be the right choice for today and tomorrow. With technology playing an increasingly important role in the success of your business, you must occasionally reevaluate your technology and IT management needs and determine whether your current MSP offers the services, tools, experience, and level of support you need to keep your IT running smoothly. The right MSP can help protect your company against IT risks and help you identify new opportunities to use technology to run your business more effectively and efficiently.

> *“Technology is the backbone of most businesses today ... They rely significantly on their IT for many different tasks and functions—and* ***if the IT fails****, it can majorly disrupt operations.”*
>
> — **JOHN KNOX**
> Director of Engineering
> and Project Management
> for CompuCom

It’s not a zero-sum decision. One analysis by International Data Corporation found that small companies that have experienced IT downtime reported that a single downtime event cost them between $82,200 and $256,000.[1] In other words, any time your entire company – or even one employee – loses work time due to an IT issue, it costs you money.

“Technology is the backbone of most businesses today,” says John Knox, Director of Engineering and Project Management for CompuCom. “They rely significantly on their IT for many different tasks and functions—and if the IT fails, it can majorly disrupt operations.”

Given the high value that efficient IT management brings to your business, it’s essential to choose your MSP thoughtfully. So, how do you know when it’s time to switch MSPs? Here are six signs it’s time for a change:

Sign #1: Your IT needs have become more complex.

If your business is growing or has been looking to adopt new technologies—whether hardware or software—your MSP must have the bandwidth and experience to scale up with you. There can be many reasons you’ve outgrown your current provider. For example, if you need to open an office or facility in a new city, you will need an MSP that can support you both remotely and on the ground in that new location. “When a company is small and starting out, they may just have a local IT shop that manages their needs,” Knox says. “But that local IT company probably won’t have the bandwidth to serve them when they expand beyond that local area or start adding employees in multiple locations.”

Moreover, the right MSP can advise you on new technologies and IT trends to help grow or improve your business. For example, a roofing company might benefit from using drones to show their clients pictures and progress of their roof job, Knox says. An MSP without the deep bench of technology experience wouldn't be able to advise that roofing company on using drones, while a larger one would have the internal knowledge and advisory services to do such consulting, as well as the partnerships with drone providers to make it easy. "A larger MSP can advise a business on automation and technological trends affecting specific industries," he says. "A smaller MSP is often just trying to stay on top of tickets and keep up with their work."

So make sure your MSP offers the advisory and consulting services you need to keep up with technology trends in your industry and maximize your opportunities.

Sign #2: Your cybersecurity technologies and protocols aren't adequately protecting you against today's biggest threats.

Cyberattacks have gotten more sophisticated and can't be stopped with just a firewall and antivirus software. Today's hackers use tactics like social engineering to take advantage of unsuspecting employees and trick them into handing over sensitive business information, personal data, and account numbers and passwords. They send seemingly trustworthy emails containing malicious links to lure employees into visiting websites that automatically download malicious software onto their computers.

Technology news site ZDNet.com predicted that some of the top emerging cyber threats in 2019 would include ransomware, cryptojacking (using malware to silently mine networks for cryptocurrency), and the targeting of "connected" devices such as security cameras or voice-activated assistants and mobile devices.[2]

Given that hackers use a wide range of methods to access data and break into companies' systems, it's important that your MSP uses a layered approach to protect your business against these threats. This should include using advanced cyber threat monitoring tools that scan emails for malicious links and deploy technologies and protocols that can protect devices when employees are at home or traveling for work.

It should also include providing comprehensive data backup and disaster recovery assistance to help prevent your business from losing access to critical system software and data in the event of, say, a ransomware attack. "There are different ways that people can get into your environment," Knox adds. "You need an MSP that has the tools and the level of sophistication to help you minimize your risks while also providing the solutions and experience to keep your business running smoothly no matter what happens."

> *"You need an MSP that has the tools and the level of* ***sophistication*** *to help you minimize your risks while also providing the solutions and experience to keep your business running smoothly no matter what happens."*
>
> — **JOHN KNOX**
> Director of Engineering
> and Project Management
> for CompuCom

Sign #3: Your current MSP has a "break/fix" mentality.

Traditionally, MSPs waited for IT problems to surface and then fixed them, Knox says. But today's most forward-thinking MSPs take a proactive approach and use remote monitoring and diagnostic tools to flag potential IT problems, software glitches, and security threats before they cause breakdowns and disrupt the business. "The future model is to monitor and fix any problem remotely over the phone," Knox says. "The worst case—simply because it takes more time—is having to send a repair person onsite."

Your MSP should use monitoring and diagnostic tools to troubleshoot problems before a major IT breakdown, which can potentially save your company time and money by helping to prevent a significant business interruption or slowdown.

Sign #4: You're not reaching experienced tech support quickly.

Time is money, and when you experience an IT problem that hinders operations, every minute of downtime or delay costs you money. When you call your MSP, you should reach someone quickly who can help resolve your issue or answer any questions.

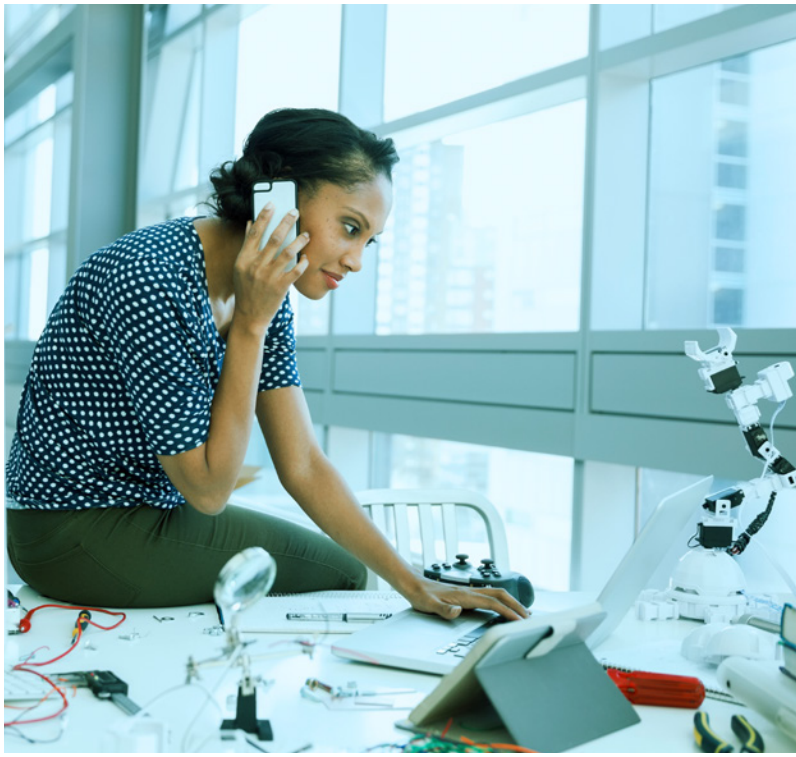
Some MSPs have receptionists or low-level tech support representatives who answer the phone and then forward concerns to experienced technicians, who respond when they're free. "The typical support model is ticket jockey: they take your information and, unless it's something very simple like a password reset, you'll have to wait to hear back from a technician," Knox says.

Your MSP should have experienced technicians answer every call because they are able to handle the vast majority of IT problems that customers have. This means there are no long wait times, and your company can get back to business promptly.

Sign #5: Managing technology vendors consumes too much of your time.

How much does your current MSP help you manage technology vendor relationships? Communicating with multiple technology vendors – whether to make a purchase order, address a problem, or manage its lifecycle – can consume hundreds of hours per year. Just one phone call can take an hour.

Some MSPs offer limited vendor management, meaning you have to take the lead in managing them yourselves. By choosing an MSP that will take care of all your vendor relationships, you and your employees can focus on your business while your MSP handles the vendor communications and management.



This can include managing and keeping track of licensing agreements and handling any service issues.

Sign #6: Your current MSP doesn't offer true around-the-clock support.

IT problems don't honor business hours. Cyberattacks often happen in the middle of the night because hackers know that's when companies are most vulnerable. An employee or team may be burning the midnight oil and suddenly the server crashes.

Being able to receive true tech support any time of day can help your business and employees reduce downtime caused by an IT problem. "We hear many complaints from businesses about other MSPs they've worked with, like 'It takes them a day to get back to us and nobody answers the phone,'" Knox admits.

An MSP that not only answers the phone but can also provide 24/7 tech support 365 days a year helps ensure that your employees aren't bogged down by IT problems regardless of when they happen.

Understanding the ROI of Choosing **the Right MSP**

It's important to understand the total value and potential savings of choosing a full-service MSP that provides the latest monitoring tools, comprehensive and around-the-clock support, and the experience that can keep your technology running efficiently and effectively while also helping you expand your technological horizons.

By choosing a more robust MSP over a smaller or more limited one, you will ultimately get back more time to focus on your business and not have to worry about your next IT problem, failure, or cybersecurity vulnerability. You will also get new ideas to take advantage of new technological solutions to compete better in your industry and become more efficient.

Choosing a proactive and full-service provider like CompuCom allows you and your employees to stay focused on your jobs and on your key goal, keeping your company successful now and into the future.

Want to learn more about the IT support, tools, services, and experience that CompuCom can offer your company that your current MSP may not provide? Contact us at **1-800-300-0983** or visit us at **smb.compucom.com** today.

[1] International Data Corporation: "The Growth Opportunity for SMB Cloud and Hybrid Business Continuity," April 2015 (https://www.carbonite.com/data-protection-resources/resource/White-paper/the-growth-opportunity-for-smb-cloud-and-hybrid-business-continuity/)

[2] ZDNet.com: "Five emerging cybersecurity threats you should take very seriously in 2019," Feb. 15, 2019 (https://www.zdnet.com/article/five-emerging-cybersecurity-threats-you-should-take-very-seriously-in-2019/)

5.17.2019

CompuCom® | MANAGED IT as a SERVICE