MANAGED SERVICES 101

An IT Resource Guide for Businesses

4 corner IT
We understand your business, not just your technology.
a wheelhouse IT company

TABLE OF CONTENTS

INTRODUCTION

It's hard to imagine what operating a business was like before the conveniences of today's modern technology. As a matter of fact, it wasn't too long ago that office desks were adorned with only a dusty typewriter, a calculator that fashioned long paper receipts, and a tiny desk calendar. There were no computers, no internet, and certainly no email accounts with 47 unread spam emails.

Information technology (IT) has certainly made operating a business much more straightforward. Over the last 30 years new features such as social media, cloud computing, and mobile applications have connected businesses more than ever and even cut down on costs. For the most part, today's executives have the luxury of spending less time on mundane tasks and more time constructively building their businesses.

But what happens when attempting to manage a dynamic IT infrastructure ends up taking away valuable time that could be used more efficiently in the business? If you're reactively working to fix IT problems only after they have surfaced, we bet you can relate to the frustration.

That's just one of the reasons you might consider partnering with a proactive Managed Services Provider.

WHAT IS THIS BOOK ABOUT?

This eBook dives into the reason that managed technology service and support is becoming increasingly important for business today, how it can prevent major breakdowns, cut expense costs, and enhance growth.

You will learn the following:

- The biggest technological threats of 2019 that negatively impact business and how to avoid them
- What Managed Services are and its common misconceptions
- The difference in cost between hiring a managed service provider vs hiring in-house
- How to hire the right MSP for your business step-by-step

Who can use the information in this book?
Whether you're a business owner, office manager, or any other valuable member of a business, this book has a wealth of knowledge in it for you. It provides an in-depth look at threats facing businesses today and addresses many of the misconceptions of Managed Services. If your business goals include thriving in areas such as security, flexibility, time management, and overall business optimization we encourage you to read on.

MODERN THREATS YOUR TECHNOLOGY IS FACING, RIGHT NOW

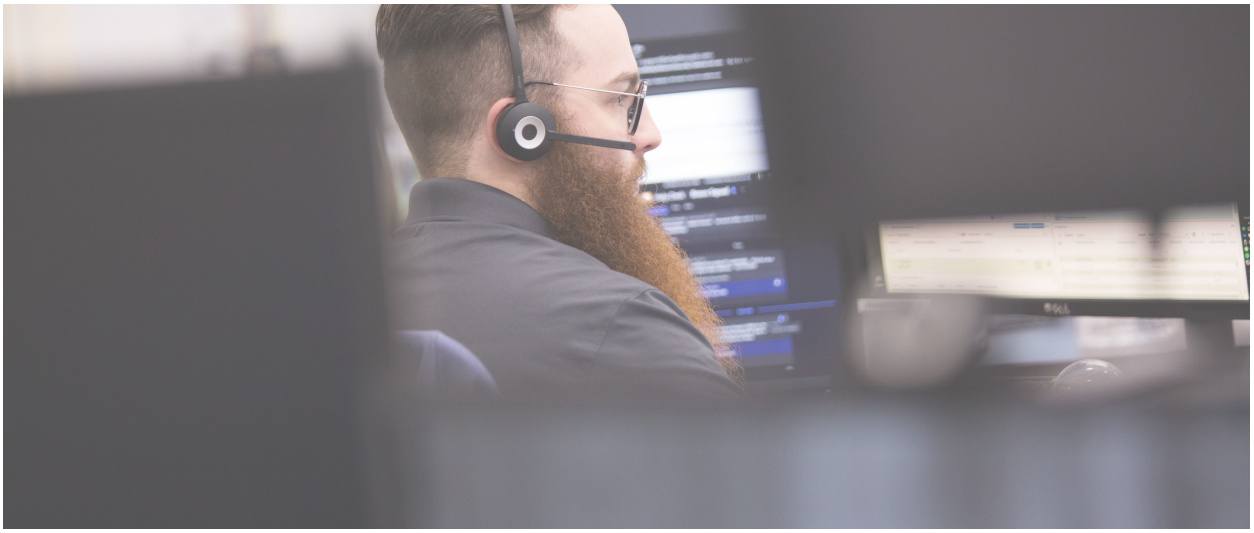
“Cyber criminals are expected to breach an estimated 33 billion records by 2023”

Cyber threats are progressively becoming more treacherous. According to a 2018 study from Jupiter Research, cyber criminals are expected to breach an estimated 33 billion records by 2023. In conjunction with this startling fact, more than half of those breaches are reported to occur in the United States alone due to the large amount of stored consumer and corporate data. [1].

Do you know how to help your business avoid the abundance of technological threats?

Are you confident in your ability to manage these emerging technologies?

Experts are discovering more and more technological hazards to look out for. Some of the top threats facing your business in 2019 include:



PHISHING SCHEMES

It's early daybreak and the world outside is still somber. You've been up for hours and anticipate the sun announcing its presence over the horizon. You sense the sticky air get a little warmer and become aware of the populous body of water nearby. You've planned this fishing day for a long time and nothing will get in your way. For hours, you'll experiment with different lures and fiddle with your technique, all in the hopes of catching a big fish.

As tranquil as that sounds, many online phishing scammers probably feel the same way when they get up in the morning. Unfortunately, YOU may be the big catch of the day! Online phishing schemes lure victims with enticing offers hoping someone will "bite" and provide the information they want.

How Phishing Schemes Get You

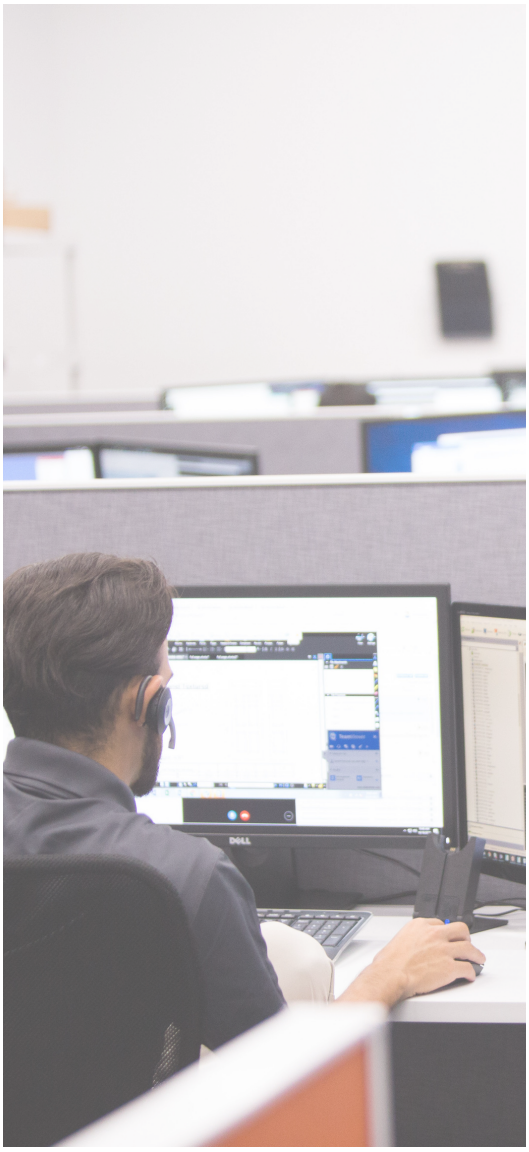
One type of phishing scheme creates fraudulent web pages that mimic legitimate web pages of companies. The counterfeit website visually copies the authentic website so that scammers can deceive victims into providing their confidential information. Frequently an unsuspecting victim will supply the information they want such as name, date of birth, social security number, mothers' maiden name, and even user names and passwords. The scammers then use this information to gain access to a victim's account and make unauthorized actions.

PHISHING SCHEMES

Phishing Schemes Target Businesses

Phishing schemes are known to infringe on businesses, conning employees into disclosing valuable company information. A Georgia man was convicted for his role in a 2012 phishing scheme that cost a total of $1.5 million to Chase Bank, Bank of America, ADP, and Branch Bank & Trust Co. [2]

These schemes have evolved to include phone, text, and even social media quizzes but email phishing schemes are still the most common of this threat. Phishing emails have become so well disguised that it can be hard for anyone to miss the signs of deception. Business email schemes grew 136% between December 2016 and May 2018 and are now estimated to exceed $12 billion, as reported by a public service announcement released by the FBI. [3].



CLOUD COMPUTING THREATS

Having access to online cloud networks has revolutionized the way business is conducted entirely. With cloud computing, computer data is stored, managed, and processed using a network of remote servers hosted over the Internet. The data is shared between permitted users who then have the capability of accessing that data on their personal devices. Cloud computing supports consistency across a business and achieves economies of scale.

While cloud computing has made facets of managing a business much easier, it also grants hackers another access point in which to gain valuable information. Ease and convenience come with risk. Widespread security and compliance breakdowns should be in a business executive's mind when adopting a cloud model.

Recognizing both the promise of cloud computing and the risks associated with it, the Cloud Security Alliance (CSA) has pioneered a list of Nine Industry-Wide Cloud Computing Threats to look out for. Members of the group who helped publish the article includes co-chairs Rafal Los of HP, Dave Shackleford of Voodoo Security, and Bryan Sullivan of Microsoft. [4]

CLOUD COMPUTING THREATS

The list of threats are as follows:

- **Data Breaches:** Having sensitive internal data fall into the hands of competitors is a business's worst nightmare. If cloud computing databases are not properly aligned at their commencement, it could allow hackers access not only to that business's data, but their consumers as well.
- **Data Loss:** Data stored in the cloud could be lost to hackers, natural disasters, or even user error.
- **Account or Service Traffic Hijacking:** Cloud computing adds a deeper layer to the landscape reached by hijackers. Once they access stolen credentials and gain entry to protected cloud data, hijackers can easily compromise the integrity of the organization.
- **Insecure Interfaces and APIs:** Cloud computing requires a set of software application program interfaces (API) that consumers use to interact with the cloud services. Therefore, the security of cloud services is wholly dependent on the security of APIs.
- **Denial of Service:** This is an attack preventing users of a cloud service from being able to access their data. It usually leaves the victim helpless and can cause a whole system slowdown.
- **Malicious Insiders:** A malicious insider is someone who has been granted access to an organization's cloud but misuses confidential information to negatively affect the integrity of the organization's information systems.
- **Abuse of Cloud Services:** Cloud computing allows small businesses to gain access to a large amount of computing power. In the same instance, what previously took hackers years to crack now takes minutes using the power of cloud servers.

NATURAL DISASTERS

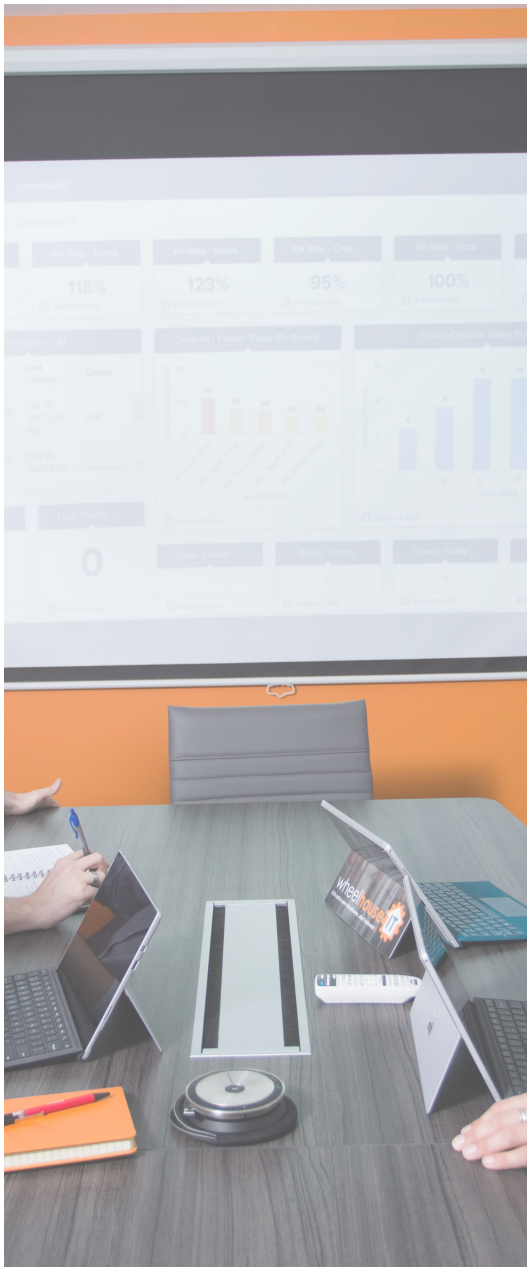
"scammers have come to realize that this is when people are the most vulnerable"

If you've turned on the news recently, it's hard to miss the barrage of reports on natural disasters occurring in the world. In the United States alone catastrophic hurricanes have devastated the south, noxious wildfires have incinerated forests out west, and polar temperatures have numbed the frostbitten north.

When we hear these types of news reports it's normal to feel empathetic and concerned. Unfortunately, scammers have come to realize that this is when people are the most vulnerable. Many scammers take advantage of natural disaster victims by posing as legitimate and reputable experts.

A very common scam after hurricanes is the assignment-of-benefits scam. Unscrupulous contractors drive around hard-hit areas and approach property owners with promises of quick repairs, waved insurance deductibles, and discounted rates.

NATURAL DISASTERS



The scammers get property owners to sign paperwork, then use that signature to collect insurance payments and disappear with the money. The state of Florida saw a total of nearly 30,000 lawsuits in 2018 alone related to assignment-of-benefits scams. [5]

Physically, natural disasters have the potential to destroy entire IT systems and infrastructure. According to the U.S. Fire Administration as reported by FEMA, there were 96,800 non-residential fires in 2016 that caused just over 2 billion dollars in damage. [6] Natural disasters affect businesses both small and large, and have the potential of disrupting operations for days or even months.

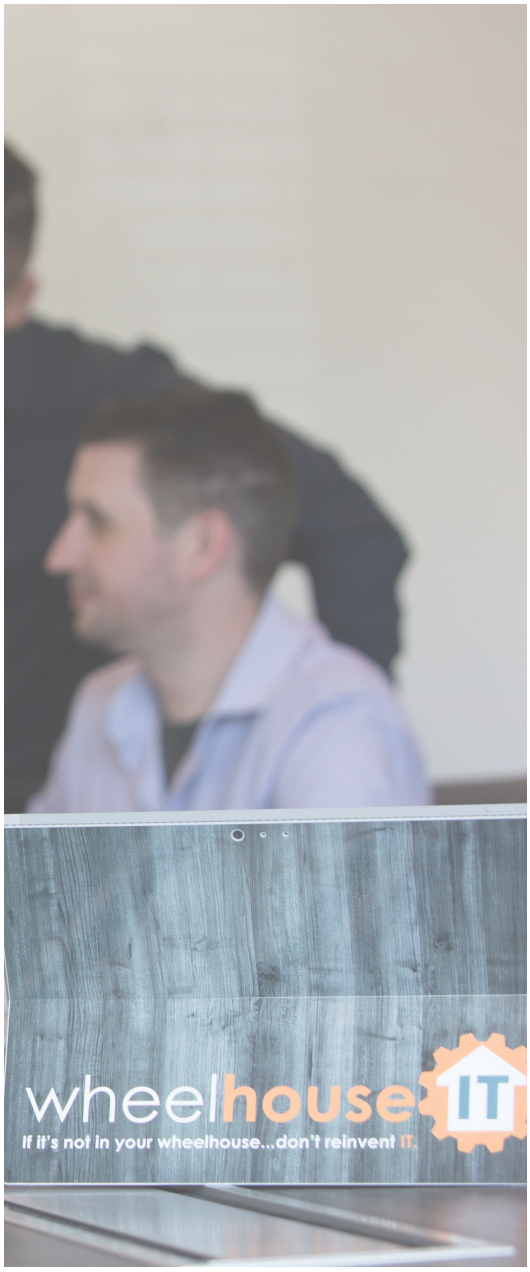
MALWARE

The term malware comes from the combination of two words: malicious and software. Malware infects devices and stops them from running properly. They steal important information, transmitting data back to the hacker.

These seven common breeds of malware have existed since the onset of the Internet. [7]

- **Virus:** Viruses are a type of malware that spreads easily and quickly through normal computer programs. Victims infect their computers by running the program.
- **Worms:** Unlike viruses, worms don't attach themselves to other programs but spread throughout a computer network. Worms copy themselves hundreds of times and spread from device-to-device stealing data, consuming bandwidth, etc.
- **Trojan Horse (Trojan):** You may have heard the famous story of the Trojan horse. The Greek army wheeled a massive, wooden horse to the gates of the city of Troy. The people opened the door to what they thought was a gift and were surprised to find Greek soldiers inside waiting to attack.
- Just like the story, Trojan malware disguises itself as a safe program. When the unsuspecting victim downloads the program, the malware gains access to their computer.
- **Adware:** Adware is a type of software that dispatches a bombardment of advertisements to their victim. Today, modern adware comes with a type of spyware attached.
- **Spyware:** Spyware "spies" on computer activity and steals personal information such as passwords, email addresses, and usernames by installing itself onto devices. Usually, this is done by key logging which is where the spyware keeps a record of everything the user types.
- **Bots:** Bots connect their victim to a host controller, or botnet. If infected by a bot, the entire control of the computer system could be lost.
- **Rootkit**: Rootkits control a victim's computer remotely. Antivirus software cannot detect rootkit software, so an IT professional will be needed to monitor this type of malware.

MALICIOUS MALWARE TO LOOK OUT FOR IN 2019



Cryptocurrency Malware

In January 2019, cyber security researchers discovered new malware that only affects Apple's operating systems. Named CookieMiner, this malware installs software that secretly mines cryptocurrency and authenticates cryptocurrency transactions on Apple devices. CookieMiner can also save victim's usernames and passwords if they are saved on their Chrome browser. **[8]**

MALICIOUS MALWARE TO LOOK OUT FOR IN 2019

Mobile Malware

According to the 2018 Symantec Internet Threat Security Report, new mobile malware increased 54% from 2016 to 2017. There were more than 24,000 malicious mobile applications blocked each day in 2017, and surely more appeared in 2018. [9]

In January 2019, a security intelligence organization called Trend Micro discovered two malicious malware apps available for download in Google Play. These seemingly useful and safe apps, named Currency Converter and BatterySaverMobi, contained malicious malware driven to steals user's information.

The scariest part was that both apps had reviews and ratings on Google Play, even boasting as high as 4.7 stars. The advanced apps were able to distinguish user's movements using the device's motion sensor data. The mobile malware only ran when the device was in motion, making sure it wouldn't be detected as malicious. [10]

THE THREATS ARE REAL – WHAT NOW?

Familiarizing yourself with these threats is a worthwhile first-step in protecting your company. Businesses hold a responsibility to protect their consumer and corporate data, so it is important to stay current and knowledgeable of these hazards. IT security is one of the most imperative obligations facing businesses during this day and age.

Are there precautions you can take to protect yourselves? Of course! Here is a list of some best practices, but this is only scratching the surface. You should also ask yourself; Am I confident that we can do this right and that it's the best use of our time as a business?

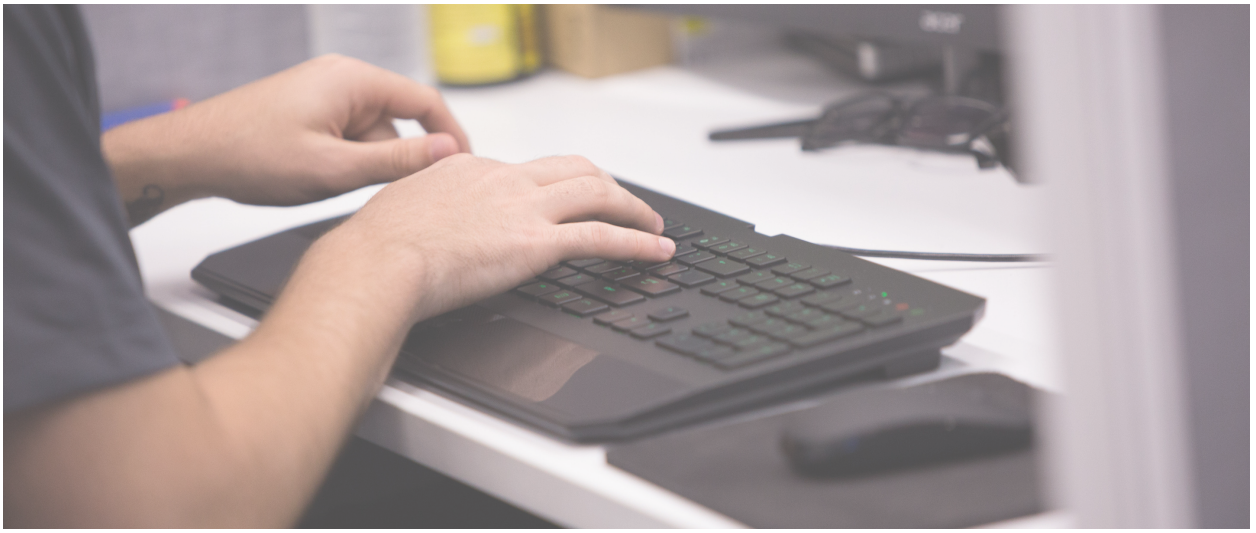
1. Have a security policy in place
2. Train your employees on how to handle suspicious emails or links
3. Screen new hires
4. Use multi-factor authentication
5. Monitor for & investigate strange activities
6. Segment LANs
7. Secure business desktops
8. Implement perimeter tools & strategies
9. Update your computers regularly
10. Choose robust passwords & change them regularly
11. Back up your data regularly
12. Encrypt your data and secure your hardware
13. Have an incidence response plan
14. Make sure your computers have updated antivirus programs

Implementing these security best practices properly is essential in today's digital era, to keep sensitive company information safe. When implementing security policies, you always want to be sure to account for both outside and inside threats, as employees can unknowingly click on the wrong thing and suddenly, you find your business in a sticky situation.

There's an Easier Way with Managed Services

Instead of dealing with the repercussions of a threat once it infiltrates your business, consider already having steps in place to prevent occurrences from happening. Instead of having to stay on top of evolving technology, let the experts get it off your plate so you can focus on what matters most to you.

Although there is no 100% foolproof way to protect against all threats, partnering with a reputable Managed Services Provider protects you more efficiently and effectively.



COMMON MISCONCEPTIONS ABOUT MANAGED SERVICES

“Your business is dependent on a reliable IT system.”

Managed Services authorizes a business to discharge its IT proceedings to a service provider.
The provider is established as their Managed Services Provider (MSP) and is accountable for constant auditing, managing, and maintenance of the IT infrastructure within a business.

MSPs materialized because of a growing need. Previously, IT maintenance was a “break it, then fix it” mentality. Deemed inefficient, as time went on leading IT support personnel developed processes to regularly come on-site and examine system logs and user information to hinder considerable complications from emerging.

When technological advances in software allowed for an affordable system capable of transforming business data into usable information, the modern-day MSP was born.

No business can bear the dangers and liabilities of relying on the old-school IT maintenance mentality.

Your business is dependent on a reliable IT system.

It is critical to prohibit complications before they disrupt the effectiveness of employees, management, or lead to customer breakdowns.

Is Managed Services Expensive?

Surprisingly no! Remote monitoring and maintenance of your business's IT systems allows major issues to be prevented. MSPs are more adept than the other companies, who just come on-site to mend the problem because they know all the ins-and-outs your business. Therefore, they have the capability of supplying your business with better service without having to charge more.

Won't I Lose Control of my Business?

The best MSPs will grant access to two-way portal that allows complete visibility of your IT infrastructure. Many will routinely produce reports for you and prove that they are consistently providing the level of service that you need. With a good MSP partner, you are always in control of your business.

Are Managed Services Less Secure?

Realistically, one of the main reasons you seek out an MSP is to offload your IT risks. Since their goal is to proactively secure workstations and networks against the ever-changing threats online, you know your MSP will have actions in place to protect you from the latest threats. Having an MSP on your team means that you can rest assured knowing that current and even future threats will be well taken care of.

COST EFFECTIVENESS OF PARTNERING WITH AN MSP

Unplanned downtime costs organizations $58,118 for every 100 users.

Pay for a Service, Not a Salary

It's no secret, your business needs IT help. Your first thought may be to hire another IT person to join the team. Before posting an ad and sitting through countless time-consuming interviews, consider the following: even if you do manage to find the most incredible IT person, no matter what, they will only be one person. Your new hire will be scheduled to work for 8 hours a day, 5 days a week.

Compare this to a partnership with an MSP who will provide your business access to an entire team of IT experts available 24 hours a day, 7 days a week. An option like this allows for limitless scalability and resources. Instead of spending money on another salary and benefits package, pay an hourly fee or service charge instead with an MSP. Overall, you'll pay less for IT services in the long run and will have a predictable monthly cost you can budget for.

Avoid Associated Costs

As your business grows and your IT needs increase, you may find yourself needing an extensive team of IT support personnel. By continuing to hire more people, taking this route will lead to additional upkeep costs. Licensing, continuing education, equipment, advanced training, and other services are not only incredibly expensive on their own, but require time from the new employees themselves.

By partnering with an MSP, your business will not need to worry about the extra costs of training new employees who, at the end of the day, are unable to guarantee the level service the way MSP can.

Reduce Costly Downtime

One of the costliest things a business can experience is an IT interruption. When an IT infrastructure goes down, work can't be done. According to a white paper written by IDC, unplanned downtime costs organizations $58,118 for every 100 users. The average employee is losing 12.4 hours a year due to server downti*m*e an*d 6.2* hours a year due to n*e*twork downtime.

Reduce sever and network downtown by more than 85 percent by partnering with an MSP. [11] An MSP will provide damage control and proactive maintenance to limit IT associated losses.

FIND THE RIGHT MANAGE SERVICES PROVIDER IN FOUR EASY STEPS

“Building a partnership by considering each other’s perspectives is an essential step.”

FIND THE RIGHT MANAGE SERVICES PROVIDER

With many MSPs out there, how will you know which provider would be a good match for your business?

Determine your Business Goals

- Identify what you like to achieve with an MSP ally. What kind of IT solutions do you undeniably need?
- Do you need to secure your networks against digital threats?
- Do you lack the expertise to quickly handle IT issues costing you time and money?
- Or, do you just need to complement your internal team with additional support?

Prior to selecting an MSP, be sure to sketch out your short- and long-term business objectives to guarantee the chosen MSP will assist in your business's growth.

Find a Local and Reputable Managed Services Provider

Although Managed Services can be done from anywhere in the world, finding a local company that provides the option of doing a physical dispatch is ideal. Therefore, while it's not necessary, choosing a MSP that is in the same city as your own business is recommended. Sometimes, you just want that one-on-one time with an expert to resolve a problem.

There's also value in examining an MSPs certifications, awards, and years of experience. While excellent customer service is attractive, half the job is still technical in nature. Find an MSP whose technical abilities leave you in awe. Additionally, find an MSP that has successful and continuous relationships with companies you know and trust.

Determine the Value Added

A favorable MSP is worth their weight in questions. They want to acquire all the knowledge they can about your business, digging deep to get a feel of your company. An excellent MSP will offer 24/7 support, both remotely and on-site. As a member of a business, how much is your data worth to you? Those who truly value their data will only accept the best when it comes to MSPs.

Building a Partnership

Building a partnership by considering each other's perspectives is an essential step. You want someone that can build a smooth path toward your business goals. Find a partner you can really work with. You are bestowing them with a serious responsibility. An ideal MSP is a clear communicator who is anxious to take your concerns seriously.

CHOOSING THE RIGHT TECHNOLOGY PARTNER WITH THE RIGHT QUESTIONS

There is a lot to consider when selecting a managed service provider that will work well with your business. Use the following questions to dig a little deeper into understanding how your potential relationship would look like:

1. How will you help us determine our priorities?

Lack of prioritization may result in spending many hours fixing vulnerabilities that have little impact on your business, while ignoring more menacing dangers.

Security assessments should present standard severity ratings and consistent read-outs, so the team knows where to prioritize effort.

2. What is your pricing structure?

Pricing and pricing structure should be transparent. The amount you pay will depend on a variety of things, including but not limited to:

- Number and type of applications you expect to test
- Number of applications that require in-depth manual testing and business logic testing
- Turn-around time you require to receive results and feedback
- If retests are included
- How frequently business or product changes will affect application security
- If read-out calls with developers are included
- Number of services & level of support needed; whether just partial support or the need for full functioning outsourced IT department.

Once you can establish your requirements, choose a provider based on expertise and methodology. A full technology partner that provides valuable insight, actionable steps and guidance may be more expensive but much more valuable than one that just hands you a report of bugs and vu*l*nerabilities with little guidance.

At the end of the day, the right managed service provider will help decrease your overall costs and increase time you can spend on other business initiatives.

3. How predictable will the budget be?

Once you agree on a price, you should be able to structure it at a predictable price. Double check that you're not paying extra for customized reports or other hidden fees that may catch you by surprise.

4. How do you test for vulnerabilities?

A combination of tools and expert manual analysis based on business context can identify vulnerabilities that automated tests alone can miss.
Look for a managed services provider that provides static (SAST) and dynamic (DAST) tests for web and mobile applications, as well as manual business logic for multiple step attacks.

A great MSP should also offer network-level assessment services. They should search for vulnerabilities in key areas such as router filtering, firewall filtering, visible network services, operating system software flaws, server application software flaws, known configuration errors, access management, and authentication controls.

5. What types of assessment tools do you use?

Some MSPs take a simplistic approach to tool-based scans. But the truth is, even in a single application, different tools can catch different susceptibilities.
Look for a managed services provider that uses a combination of commercial, internally developed, and open-source tools so that they can utilize the most appropriate testing techniques for the application being tested.

6. What solutions do you provide that will help our business reach our future goals?

A good MSP will strive to be your technology partner and play a key role in the success of your business. They will look holistically at your business to find opportunities for optimization, so that you can streamline and protect your business so that it can continue to scale.

FINAL THOUGHTS ON MANAGED SERVICES

WheelHouse IT is an MSP that provides a wide range of support for client infrastructure, while proactively securing workstations and networks against the ever-changing threats online, so you can focus on running your business.

Throughout this eBook you've learned how to mitigate different IT issues, reduce risk, remain in control, and grow your business to new heights. Finding the right MSP will ensure your business has the flexibility it needs to thrive, while giving you the peace of mind to focus on growing your business.

Why WheelHouse IT?

WheelHouse IT is an MSP that provides a wide range of support for client infrastructure, while proactively securing workstations and networks against the ever-changing threats online, so you can focus on running your business.

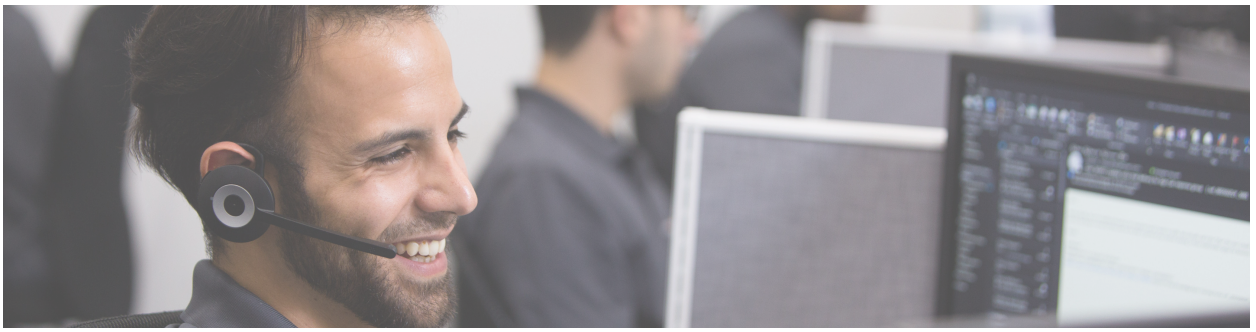
Our Clients are Our Partners, and Their Success is Our Success

We partner with strong companies such as Microsoft, Amazon, Dell, Cisco, and many others to help implement the right technology for your success. To achieve a common goal, we fuse together our laser-focused passion for technology with our multi-environment experience to enhance our client's already proven business models.

Our approach includes stabilization, support, management, and the transformation of our partners in this ever-evolving world of Information Technology.

What we do to align with your business.

- We learn your business and vision and align the right technology to support that vision.
- We strive to always be on the leading edge of new technology.
- We are a true caring partner and place high priority on our customers' experience.
- We take a family-oriented approach to customer support.
- We provide 24/7/365 support and peace of mind to our customers
- We combine the capabilities of an enterprise class service with the personalized attention of a local provider, serving Ft. Lauderdale, New York, Los Angeles, Iowa and Arkansas.
- Our solutions guarantee the security and availability of your backed-up data.



In an industry that feels very commercial on the surface, if done correctly, Managed IT includes so much more than just support. We're talking about disaster recovery, employee training, VoIP and telecom consolidation, Microsoft collaboration tools, SaaS, FaaS, WaaS, and the backbone of a friendly, knowledgeable support team more than 50 large across a network of locations. A support team that wants to help you solve problems and prevent others.

Find out why we are ranked 127th in the world in the Managed Services industry by MSPmentor.

LET US TRANSFORM YOUR RELATIONSHIP WITH I.T.

WheelHouse IT can help you stabilize, support, manage, and transform your business with our Managed IT Services and solutions.

Contact WheelHouse IT

wheelhouseit.com
(877) 771-2384
sales@wheelhouseit.com

FORT LAUDERDALE
2890 West State Rd. 84
Suite 108
Fort Lauderdale, FL 33312
(954) 474-2204

NEW YORK
1866 Seaford Ave
Wantagh, NY 11793
(516) 536-5006

LOS ANGELES
529 S. Broadway St.
Suite 4004
Los Angeles, CA 90013
(323) 977-6400

SOURCES

[1] “10 cyber security facts and statistics for 2018,” Norton.com, 2018. [Online]. Available: https://us.norton.com/internetsecurity-emerging-threats-10-facts-about-todays-cybersecurity-landscape-that-you-should-know.html. [Accessed 12 February 2019].

[2] “Georgia Man Convicted in New Jersey for His Role in Phishing Scheme,” FBI.gov, 27 June 2012. [Online]. Available: https://archives.fbi.gov/archives/newark/press-releases/2012/georgia-man-convicted-in-new-jersey-for-his-role-in-phishing-scheme. [Accessed 12 February 2019].

[3] “Business E-mail Compromise the 12 Billion Dollar Scam,” Federal Bureau of Investigation, 12 July 2018. [Online]. Available: https://www.ic3.gov/media/2018/180712.aspx. [Accessed 12 February 2019].

[4] “The Notorious Nine: Cloud Computing Top Threats in 2013,” Cloud Security Alliance, February 2013. [Online]. Available: https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf. [Accessed 12 February 2019].

[5] O. Blanco, “Protect Yourself from Post-Storm Scams,” Consumer Reports, 20 October 2018. [Online]. Available: https://www.consumerreports.org/scams-fraud/protect-yourself-from-post-storm-scams/. [Accessed 12 Feburary 2019].

[6] “Nonresidential Building Fire Trends (2007-2016),” FEMA, May 2018. [Online]. Available: https://www.usfa.fema.gov/downloads/pdf/statistics/nonres_bldg_fire_estimates.pdf. [Accessed 12 February 2019].

[7] “What are Viruses and Malware?” BBC Bitesize, [Online]. Available: https://www.bbc.com/bitesize/articles/zcmbgk7. [Accessed 12 February 2019].

[8] W. Suberg, “CookieMiner Malware Tries to Hack Mac Users’ Cryptocurrency Exchange Accounts Report,” Cointelegraph.com, 1 February 2019. [Online]. Available: https://cointelegraph.com/news/cookieminer-malware-tries-to-hack-mac-users-cryptocurrency-exchange-accounts-report. [Accessed 12 February 2019].

[9] “ISTR: Internet Threat Security Report,” Symantec, 2018. [Online]. Available: https://www.symantec.com/security-center/threat-report. [Accessed 12 January 2019].

[10] K. Sun, “Google Play Apps Drop Anubis Banking Malware, Use Motion-based Evasion Tactics,” TrendMicro.com, 17 January 2019. [Online]. Available: https://blog.trendmicro.com/trendlabs-security-intelligence/google-play-apps-drop-anubis-banking-malware-use-motion-based-evasion-tactics/. [Accessed 12 February 2019].