MANAGED SERVICES 101

An IT Resource for Business Owners

Centre TECHNOLOGIES

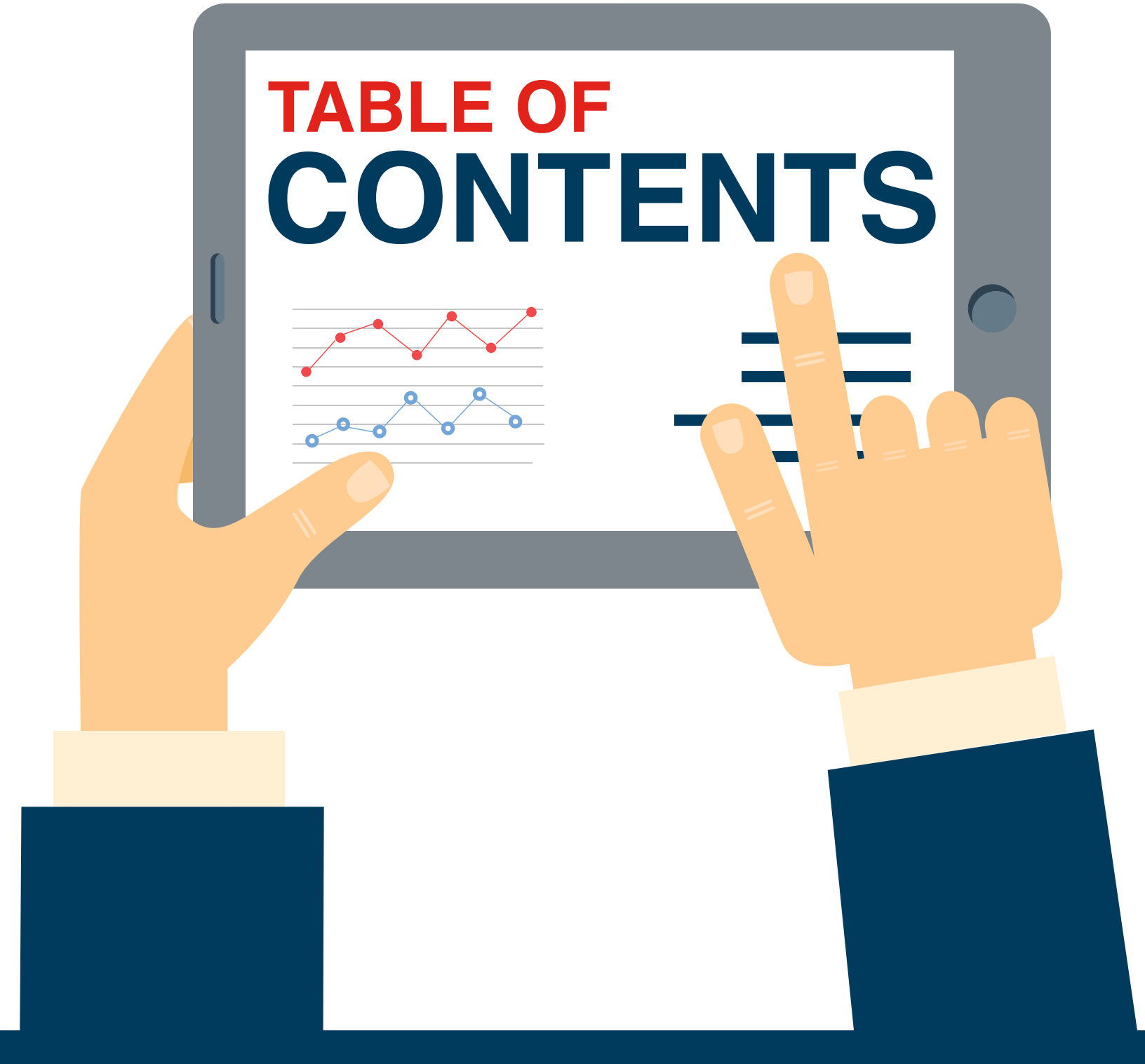
TABLE OF
CONTENTS

Introduction

Technology is a tool with two sides: one side has the power to slash through limitations and take your business to new heights, while the other side is poised to make your business more vulnerable to threats.

The question is: Do you know how to wield it? If you're not confident in your ability to handle emerging technologies to benefit your business, do you know what resources you can leverage to keep your competitive advantage?

With this book, you get "must have" information about a solution that many businesses overlook. If your business has concerns with the lack of:

- Flexibility
- Growth
- Peace of mind
- Time to focus on your core business

…you need the information in this book. Businesses that leverage a Managed Services offering ultimately reduce their risk, offload the bulk of their IT pains, while still remaining in control of all of their data. The right IT solution will support a business, and many businesses who would have otherwise benefited from Managed Services are missing out due to common misconceptions.

What is This Book About?

This book is a resource for businesses who need to understand the threats facing their business, as well a possible solution to help them fight back.

- Learn about modern technology threats facing your business right now in 2015.
- Discover an easy way to free up your time to focus on your business.
- Find out how to protect and enhance your network to take your business to new heights.

Who is This Book For?

Whether you're a Managed Services neophyte or an experienced IT veteran, this book contains something for you. It involves an in-depth look at the current and impending threats on the technology landscape and dispels common misconceptions about what Managed Services are. In particular, this book will be most helpful to:

- Small business owners
- Mid-size business owners
- Newly launched businesses

Any business, or business owner, who is looking for a way to remediate their IT pains and spend more time concentrating on their business, will benefit from the information in this book.

Modern Threats Your Technology is Facing, Right Now

As technology becomes more and more engrained in our daily lives, so will technology-related threats. Run-of-the-mill firewalls and antiviruses can only do so much to protect your network.

New, Malicious Breeds of Malware

"Malicious software" has been a persistent sore spot for technology, and it has only gotten more malicious in recent years. For those unfamiliar with the word, malware is an umbrella term to describe any software created to infiltrate your computer or network without your consent.

Common Malware Classifications

These seven types of malware have been present since the inception of the commercial internet. They are designed to exploit your network's (and sometimes, your employees') vulnerabilities.

Viruses: software that can copy itself and spread to other computers by attaching themselves to programs. Victims infect their computers when they try to execute the program.

Trojans: a malware that can disguise itself as a normal program. Unsuspecting victims download and launch the file, giving the attacker access to your computer.

Worms: software that exploits vulnerabilities and spreads throughout a computer network. Worms can spread independently and deliver malicious code that can steal your data, consume bandwidth, etc.

Adware: software that delivers unwanted barrages of advertisements. Many modern adware comes with some form of spyware attached.

Spyware: software that, per their name, spies on a victim's computer activity. Spyware can harvest data, monitor user activity, even change your computer's security settings without your knowledge.

Rootkit: software that can control a computer remotely. Traditional antivirus software cannot remove or detect rootkit software, so you will need the help of an IT professional to monitor, report, and remediate this type of malware.

Bots: self-propagating software that connects you (the host) to another controller, or "botnet." If your computer or server is infected by a bot, you can lose control of your system.

The best practice is to avoid malware entirely with preventative measures.

- Keep your operating system updated.
- Always keep your antivirus and scanning software up-to-date.
- Train your employees not to open unfamiliar email attachments.
- Don't let your employees download unfamiliar files from the internet.
- Install and/or keep your firewall updated.

However, even when you implement best practices, the task of keeping your organization safe from malware may still be a daunting job for even the most cautious of organizations. Essentially, you must also pose this question: If these are the threats of the past and present, what malware threats are you facing in the very near future?

2015 Malware Forecasts

Ransomware

Ransomware is a specific type of malware which restricts your access to your own documents and files. As indicated by its name, ransomware takes your data and demands that you pay a fee to the attacker to release them.

An early form of ransomware, Cryptolocker, successfully stole more than $100 million dollars [1]. McAfee Labs, a division of Intel, predicts that ransomware will become more sophisticated in 2015 and will be able to ransom your data from the cloud and mobile [2]. Like other types of malware, train your employees not to download unfamiliar files and internet attachments.

DDoS

Distributed denial of service (DDoS) attacks are neither new nor going away any time soon. This type of malicious software disrupts websites by assaulting them with a barrage of traffic from multiple sources. This overwhelms the website's server, and it becomes completely unavailable to website users. Many businesses fell victim to DDoS attacks in 2014 including Feedly, Meetup, the World Cup Website, and Vimeo [3]. Like Ransomware, many DDoS propagators demand payment to cease the attack.

Experts predict that the low-cost and high efficacy of a DDoS attack will only make it a more popular choice for hackers in 2015. In fact, DDoS attacks will continue to get more complex when used in conjunction with botnets and other forms of malware.

Removing DDoS malware gets more difficult the deeper it gets into your network. Your business cannot afford the downtime loss if your website server gets attacked. Your customers will just move to another website to conduct their business. Mitigate a DDoS attack with preemptive strikes- keep your firewalls, scanners, and OS up-to-date. If your system gets attacked, you will have to get emergency services from an IT solutions specialist.

Hackers and Security Breaches

The number one tech news that captured every business's attention in 2014 was high-profile security breaches. Large retailers suffered data loss and humiliation at the hands of hackers with losses easily topping into the millions [4].

- Target
- Home Depot
- JP Morgan Chase
- Gmail
- EBay
- Sony PSN

2015 security trend reports say that businesses have a lot to worry about this year. Hackers are refining old tricks and developing entirely new ones to breach your defenses and wreak havoc on your network and business. Here are the top five tactics you should look out for this year:

Social Engineering: Social engineering has been a typical hacking tool for many years [5]. The hacker sends an email, posing as a legitimate party to gain you or your employees' trust. They request specific information about your network, login credentials, and possibly even financial information to process a payment. They then use this information to infiltrate your network or directly steal from you. Social engineering will continue to be a threat to your business as hackers develop better ways to disguise themselves.

Third Party Hacks: A third-party hack ultimately lead to Target's data breach [6]. Even though your business's network may be secured, you also need to make sure that your partners' networks are secure too. Hackers can gain access to your network by attacking a less-secure business that you work with.

Cyber Espionage: The 2015 McAfee Labs Threat Report predicts that cyber espionage will only increase. 11% of perpetrators will be involved with organized crime and will target wealthy individuals and organizations [2].

Mobile Attacks: If your business uses mobile devices as a critical part of your organization, be prepared to be targeted. The McAfee Labs report predicts that hackers will take advantage of the lack of regulation in mobile app stores to try to get access to your device and the information in it [2].

ATM and POS Attacks: ATM's and Point-of-Sale (POS) systems will remain a target of exploitation, and experts predict that this trend will only rise in 2015 [7]. POS's, in particular, have specific vulnerabilities that allow hackers to siphon card data directly from the POS as it transfers data to the retailer network.

Natural Disasters and Catastrophic Data Loss

Businesses in Texas and Louisiana, and throughout the Gulf Coast, have to deal with the same threat every year: The Atlantic Hurricane Season. Between June 1st and November 30th, businesses remain on edge just in case another hurricane devastates their city.

Businesses who don't have a disaster recovery and business continuity plan in place stand to suffer from $84,000 to $90,000 dollars in hourly downtime loss [8].

Innovation

Innovation brings challenges for IT. Employee and customer expectations change as technology changes, and many businesses feel the strain of these new demands.

Poor MDM Strategy

You've probably already been introduced to the idea of BYOD, or bring-your-own-device. In order for BYOD to be successful, your organization needs to have a strong MDM strategy to mitigate the risks of mobility. Workplace mobility is the next great workforce innovation, but if you don't have the right technical and governance measures in place, your BYOD policy can severely damage your organization [9].

- Security breaches via your employee's mobile device
- Data loss and privacy compromise if a device is lost or stolen.
- Disagreements over the regulation of employee privacy and ownership.

The Threats are Real – What Now?

2015 and beyond will be ripe with emerging threats [10]. Instead of dealing with them after you've become a victim, consider the amount of time, money, and stress you can save if you prevent them entirely. Imagine a solution that provides enterprise level service with local support that protects your business from emerging IT threats. More importantly, what if protecting you from threats was only part of an overall solution?

This is where Managed Services comes in.

Common Misconceptions about Managed Services

What is Managed Services?

Managed services allow businesses, of any size, to offload their IT risks to a managed services provider, or MSP. In this type of arrangement, a business pays the MSP to deliver support and service within a specific contractual SLA, or service level agreement.

For example, if the MSP's SLA for a non-critical helpdesk ticket is 24 hours, then they must respond to the ticket within that time period. A good MSP should be able to deliver service well within their contractual SLA.

Why Does a Company Sign-up for Managed Services?

A business signs up for Managed Services for many reasons.

1. Continuous technical problems.
2. Lack of a dedicated IT department.
3. IT department staff augmentation.
4. Unpredictable IT budget.
5. Help investing in and implementing innovation.

These reasons usually boil down to one: the need for a business to have more flexibility, growth, and peace of mind.

Dispelling Misconceptions

Misconception #1: Business Lose Control of their Infrastructure

Most MSP's will give you access to a two-way portal that will give you complete visibility into your infrastructure and their management of it. They should automatically generate reports for you and be able to prove that they are delivering on their SLA. With a good MSP, you are always in control of your infrastructure.

Misconception #2: Lose/Reduce Your Staff

The best MSP's are designed to augment your staff, not replace it. If you already have an IT staff in place, you are adding valuable IT professionals to your team to help ease the burden from your staff's shoulders. This helps your employees refocus their energies to concentrate on your business, not your everyday technology problems.

Misconception #3: MSP's are Costly

The maturation of new technologies, like cloud and virtualization, has changed the way MSP's package their services. Many MSP's will charge either per user or per device. A good MSP will ensure that their charges are transparent, proving the value of your investment. Additionally, with an MSP, you are using many of their resources, instead of investing in your own, reducing your overall capex.

Misconception #4: MSP's are Nothing More Than an External Help Desk

While a large part of an MSP's function is to provide support, a good MSP will often provide much more. Their technologies and methodologies can help your business meet your compliance objectives, improve your security, enhance your network, and provide technical expertise to solve your long-term problems.

Misconception #5: Managed Services is Less Secure

The point of seeking help from managed services is to offload your IT risks. MSP's understand this, and they are often more secure as a result of this. They handle the accounts of several businesses at once, and they cannot afford to let any of them be compromised by malware or hackers. They will consistently patch your software, keep your firewalls up to date, update your antivirus, and constantly monitor your network for signs of intrusion.

What Services Should an MSP Provide?

Support

The most basic service an MSP should provide is help desk support. They should be a dedicated IT resource that receives and resolves a myriad of IT problems. Ideally, you should partner with an MSP that offers remote and on-site support 24x7, 365 days a year.

Remediation

When a help desk ticket is placed, you should expect a prompt response from your MSP. The solution they provide should be a long-term resolution of your acute problems. You could say that an ideal MSP will take a "no Band-Aids" approach to troubleshooting your IT pains.

Maintenance

The first two features of managed services are only the surface of a deeper offering. These next four features are where you should experience the bulk of your value. An MSP should provide your business with patching, proactive software updates, and proactive antivirus updates. The users in your business should experience as little problems as possible once you offload your IT pains to Managed Services.

Monitoring

Do you remember the threats discussed in Chapter 1? It is the MSP's job to monitor the health and performance of your servers (physical and/or virtual), and spot issues before you've been affected. Many MSP's will install a remote management software into every workstation for a holistic view of your infrastructure.

Reporting

You should always be closely involved with your own technology. Even if you offload the risks to your MSP, you should never feel as if you've lost control. This is the most common misconception about Managed Services. Your MSP should provide you with asset inventories, reports, and complete visibility of your IT environment.

Security

As discussed, there are many threats facing the modern business's network. Your MSP should be responsible for ensuring, beyond all doubt, that your network will be secured. They should provide protection against malware, network breaches, and cloud breaches. In short, if an MSP cannot provide comprehensive network security, you have no reason to partner with them.

A Final Note about Value

At the bare minimum, your MSP should provide support and remediation. However, you will not be getting any true value from their services if they don't also provide security and maintenance. Fewer companies, still, also provide around-the-cloud monitoring and transparent reporting.

Ideally, you should partner with a Managed Services provider who provides all five services and enterprise-class hardware and software to support your growing business. This next section will help you find a local MSP that fits the needs of your business.

Step-by-Step: How to Find the Right Managed Services Provider

It's not too difficult to find an MSP. A simple internet search can bring up several local, relevant prospects.

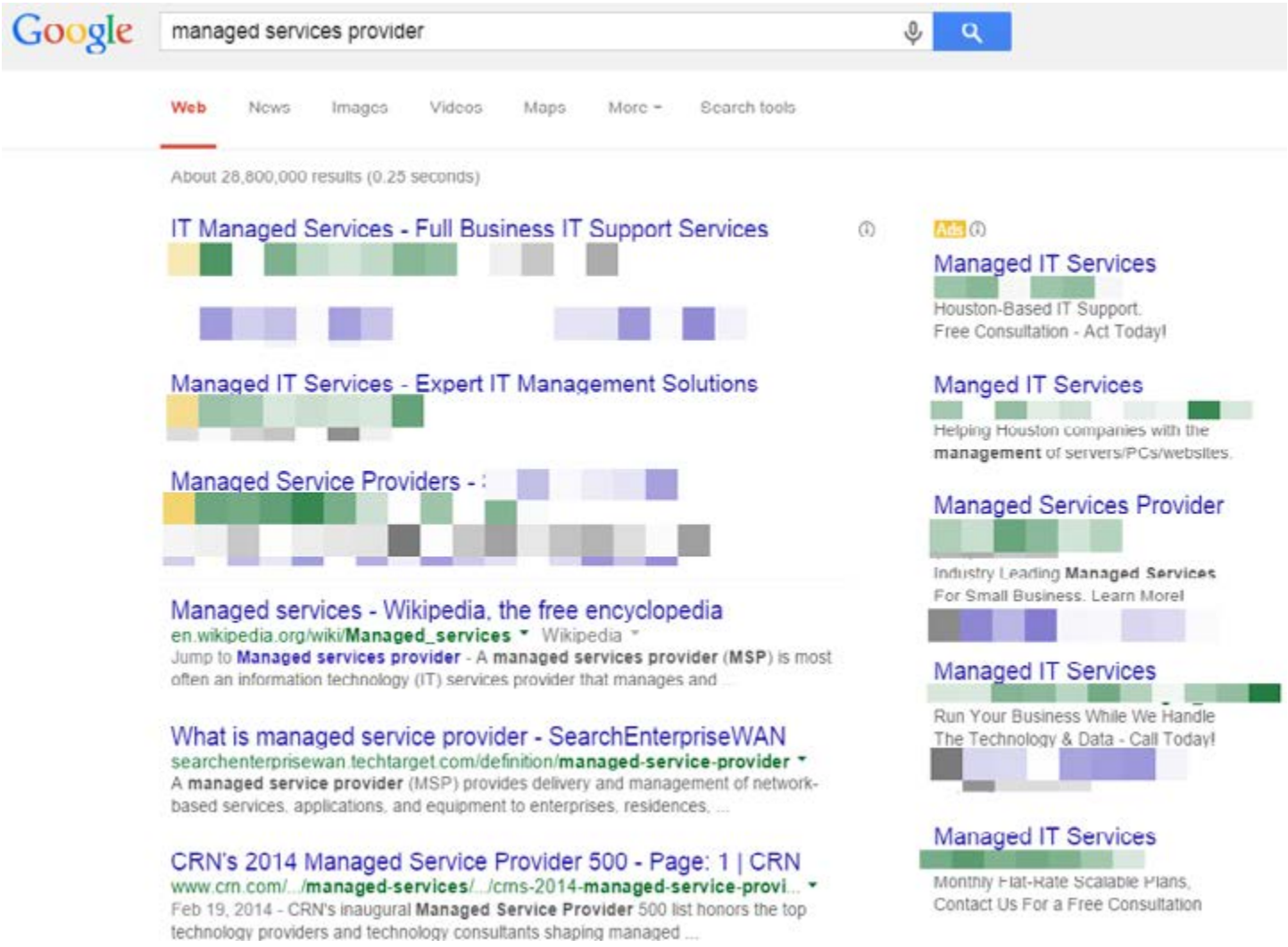

Figure 1: Google Search "Managed Services Provider."

However, this poses an immediate problem: how do you know which MSP is right for your business? Which IT solutions company will provide your business with adequate support, remediation, maintenance, monitoring, reporting, and security?

Step 1: Identify Your Business's Goals

Identify your business's goals: What do you want to achieve with Managed Services? While it may be tempting to skip this step and jump right into the search for a provider, it's important to establish your goals first.

- Do you lack the technical expertise to handle your IT problems?
- Do you want more protection against network security threats?
- Do you need additional technical staff to help your in-house staff complete a project?
- Do you need a long term or short term managed services partnership?

When you delegate your IT matters to an MSP, you should always have a sense of "what's next" in mind.

Step 2: Find a Provider That Offers Enterprise Class Service

This eBook uses the word “enterprise class service.” In the simplest sense, this means providing critical technology services that apply to every user in the entire organization. National MSP’s offer tools like:

- Multiple network operation centers (NOC’s)
- Help-desk/End-user support
- Delivery of services
- Technology consultation
- Analysis and reporting
- Hardware and software life-cycle maintenance
- Software configuration and core application integration
- Quality, security, assurance, and compliance (QSAC)
- Backup and discovery recovery

Enterprise class services even have the capability to support their end users within a disaster area which, for businesses throughout the Gulf Coast, can make or break their business.

Step 3: Find a Local Service Provider

Managed Services could easily be a remote service delivered to your business from anywhere in the world. While you could easily get service from a national company, for optimal service, pick a local MSP that gives you the option of physical dispatch. Choose a provider with an office in the same city as your business (or reasonable vicinity) for best results.

Why do you need a local service provider?

Some of your problems might not be resolved through remote means alone, and you may need a certified technical professional to visit your physical business to resolve some of your IT problems. Their presence onsite at your business in invaluable and gives them the ability to see what your users see. Only a local MSP has the capability to work with your end users one-on-one to resolve problems.

Step 4: Find Out Who Their Partners Are

All MSP’s work with IT manufacturing partners. You can expect them to work with companies like Citrix, VMware, Dell, etc. Evaluate the quality of their partners. Choose a Managed Services provider that works with best-of-breed partners. This way, you can enjoy enterprise-class products as a part of your infrastructure without the capex required to obtain them yourself.

Step 5: Find Out How They Provide Value

More than a price tag, the value of a managed services company is comprised of these equal parts:

- Their methodologies
- The technical and customer service expertise of their employees
- Their partners

MSPs usually charge their services per device/workstation or per user. Determine which pricing structure will be more cost-effective for your business. The simplest and most strategic way to save money on your monthly MSP bill is to find a provider that charges per workstation.

If you select a provider that charges per user, you might spend money on users that may never require an IT resource. Additionally, you can regulate your workstations with more ease and accuracy than you can individual users.

Final Thoughts on Managed Services

Throughout this e-book, we discussed:

- Flexibility
- Growth
- Peace of mind
- Time to focus on your core business

Managed Services has the ability to address all four concerns. An MSP gives your business the flexibility it needs to grow, while giving you the peace of mind to focus on your core business.

Why Centre Technologies?

1. Centre is an IT solutions industry leader that never stops innovating and never stops investigating new ways to mitigate new threats.
2. Our proven methodologies ensure ultimate safety and performance for your network.
3. Our solutions guarantee the security and availability of automatically backed up data.
4. We address common misconceptions about Managed Services and establish a partnership based on business value.
5. We work closely with our Managed Services clients to help them reach their business goals.
6. We provide local, enterprise-class support to businesses throughout Texas and Louisiana.
7. We pass the value of working with our best-of-breed partners to you and your business.
8. Our certified and experienced IT professionals consistently meet and exceed our contractual SLA's.
9. Our services combine the capabilities of an enterprise class service with the personalized attention of a local provider; the only MSP in Texas that can provide the best of both.
10. We offer multiple network operation centers and redundant tools from two separate geographic locations to ensure 24/7/365 support.
11. Our core focus is to provide nothing short of the best value for your IT investment in the industry.

Contact Centre Technologies

If you want to personally explore what value Centre's Managed Services can bring to your business, contact us directly.

Phone: 281-506-2480
Address: 480 N. Sam Houston Parkway E. Suite 100, Houston, TX 77060
Website: www.centretechnologies.com

About Centre Technologies
Centre Technologies is a privately-owned, leading IT company that provides IT solutions for businesses of all sizes in Texas and Louisiana. Since 2006, Centre Technologies has combined technology with business insight to create a customized set of services as unique as the organizations they were created for. Their approach to enhancing businesses with IT operates under the principle that, "Technology is the Centre of every business."

Bibliography

[1] A. Press, “Hacking Scheme That Stole Millions Busted by U.S.,” NBC News , 2 June 2014. [Online]. Available: http://www.nbcnews.com/news/crime-courts/hacking-scheme-stole-millions-busted-u-s-n120946. [Accessed 13 January 2015].

[2] M. Labs, “Infographic: McAfee Labs 2015 Threats Predictions,” McAfee.com, 9 December 2014. [Online]. Available: http://www.mcafee.com/de/security-awareness/articles/mcafee-labs-threats-predictions-2015.aspx. [Accessed 13 January 2015].

[3] S. Perez, “Feedly, Evernote And Others Become Latest Victims Of DDoS Attacks,” Tech Crunch, 11 June 2014. [Online]. Available: http://techcrunch.com/2014/06/11/feedly-evernote-and-others-become-latest-victims-of-ddos-attacks/. [Accessed 13 January 2015].

[4] D. McCandless and T. Evans, “World’s Biggest Data Breaches,” VIZSweet, September 2014. [Online]. Available: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/. [Accessed 13 January 2015].

[5] J. Pepitone, “The Year in Cybersecurity: 5 Threats to Watch in 2015,” NBCNEWS.com , 30 December 2014. [Online]. Available: http://www.nbcnews.com/tech/security/year-cybersecurity-5-threats-watch-2015-n270271. [Accessed 13 January 2015].

[6] H. Ellyatt, “Top 5 cybersecurity risks for 2015,” CNBC.com, 5 January 2015. [Online]. Available: http://www.cnbc.com/id/102283615. [Accessed 13 January 2015].

[7] GReAT, “Kaspersky Security Bulletin 2014. Predictions 2015,” Securelist.com, 1 December 2014. [Online]. Available: http://securelist.com/analysis/kaspersky-security-bulletin/67864/kaspersky-security-bulletin-2014-predictions-2015/. [Accessed 13 January 2015].

[8] Vision Solutions, “Assessing the Financial Impact of Downtime,” Vision Solutions Inc., Irvine, 2008.

[9] E. Burns, “8 BYOD PREDICTIONS FOR A MOBILE 2015,” CBR, 19 December 2014. [Online]. Available: http://www.cbronline.com/news/tech/hardware/desktops/8-byod-predictions-for-a-mobile-2015-4473898. [Accessed 13 January 2015].

[10] K. Zetter, “The Biggest Security Threats We’ll Face in 2015,” wired.com, 4 January 2015. [Online]. Available: http://www.wired.com/2015/01/security-predictions-2015/. [Accessed 13 January 2015].