TechSage Tech Talk

TechSage Solutions

Insider Tips to Make Your Business Run Faster, Easier and More Profitable

We love technology and We love helping people.

Give me a call to find out whether we can help you better secure your data and get more out of technology.

-John Hill
Founder CEO

Help Your Business Thrive With Co-Managed IT Services

Over the past few years, awareness about IT services has significantly increased. Businesses of varying sizes recognize the need for and importance of utilizing IT services to protect sensitive data, keep day-to-day operations running smoothly, increase productivity throughout various departments and stay up-to-date with the most recent technology trends. Without IT services, companies put themselves and their clients at risk. So, if you're looking to add these kinds of services to your business – or are in need of an update – you may wonder what your options are.

IT Services Providers Available For My Business

When it comes to adding IT services to your business, there are essentially three main options. Sure, you could try incorporating new practices yourself, but this will take you away from other projects, so it's best to turn to the professionals for what you need. One option that's becoming rare is hiring an in-house IT team. This allows you to have an IT professional or team working at your business on a daily basis. They can handle most minor tech issues in a timely manner and will always be available to answer questions.

You'll also maintain control over the different practices, programs and

protections that are in place.

Another option is to hire a managed services provider. MSPs come with a host of benefits and take much of the stress out of your IT needs. MSPs can help your systems operate more efficiently, reduce costs related to managing IT software, improve your cyber security efforts and answer any questions you may have. MSPs are third-party companies that must adhere to certain industry standards, but they don't work directly out of your business. This means if you utilize MSP services, you will relinquish many of your IT decisions and responsibilities to the experts.

Get More Free Tips, Tools and Services At Our Website: *www.techsagesolutions.com/securitytips/*

The final option is the best of both worlds, and it's called co-managed IT services. This option allows you to outsource some of your more critical IT functions while still maintaining an in-house team. You can have the outsourced IT service manage your network infrastructure, which ensures your routers, firewalls and other network devices continue to work correctly. With co-managed IT services, an MSP can manage and monitor your data backup and recovery solutions, cyber security practices and defenses, cloud management and optimization and even IT project management. They can be available at all hours of the day to offer support and guidance for any needs you may have. And you'll get to experience all these benefits while still maintaining an in-house IT department. Your in-house team can handle all quick problems and offer immediate assistance while the MSP handles everything else.

The Benefits Of Co-Managed IT

Now that you're more familiar with co-managed IT services, you might wonder what the benefits are so

> **"With co-managed IT services, an MSP can manage and monitor your data backup and recovery solutions, cyber security practices and defenses, cloud management and optimization and even IT project management."**

you can determine if it's the right fit for your business. One of the first benefits is that co-managed IT can save businesses quite a bit of money. Maintaining a full in-house IT department or depending on an MSP for every IT need can get expensive. But by outsourcing specific functions, you can lessen the number of people on your in-house IT team, and many MSPs provide differently priced packages depending on your company's needs. This will help you find the right balance that also fits your IT budget. You'll have more control and flexibility over your IT infrastructure as well, so you can choose who handles each responsibility and what functions the third-party team manages.

Another great benefit you'll gain from a co-managed IT service is a double layer of expertise and security. Not only will you have a team on the ground able to provide quick fixes to common problems, but you'll also have an MSP holding down your back line and ensuring everything else runs smoothly. Both your in-house and outsource team will have experience and knowledge to guide you through any dilemma that may arise.

No matter what the IT needs are for your business, there's an IT option that's bound to help your business find more success. We can help if you're still unsure which option is best for you and your business. Once your IT needs are met, you can focus your attention on the daily operations of your business and find new ways to become more profitable and efficient.

A Business Leader's Quick Guide to AI

Artificial intelligence is quickly transforming the world. As a business leader, it is essential that you understand the best practices, benefits and ways you can leverage AI for your business.
Businesses implementing AI see a significant improvement in customer satisfaction and greater clarity in sales and marketing decisions. Automating routine tasks also allows employees to dedicate more time to business-critical tasks.

Download the quick guide to AI at:

www.techsagesolutions.com/Guide-AI/

HOW TO USE CHATGPT AT YOUR BUSINESS RESPONSIBLY

ChatGPT has revolutionized the way businesses interact with their customers. It has also affected how they get things done. Teams are using it for everything from emails to generating ideas for product names.

The tool's personalized and informative responses in real-time definitely draw you in. But integrating ChatGPT into your business operations requires careful consideration. You want to ensure that things don't get out of hand with employees using the tool irresponsibly.

- Understand ChatGPT's Weaknesses
- Define ChatGPT's Role
- Consider Customer Privacy
- Ensure Human Oversight
- Integrate ChatGPT Into Your Existing Customer Service
- Measure Performance and Optimize
- Be Transparent About Using It

Become Better At Hiring And Coaching

BY AVOIDING THESE 3 MISTAKES

Leaders make common mistakes with job descriptions when hiring and reviewing performance. The consequence is an increased probability of hiring mistakes or providing someone with useless performance feedback. Leaders often fall into this trap to avoid accountability or because they fear a performance expectation is flawed.

Most of these errors are entirely preventable. Here are three mistakes every leader should watch out for.

Describing A Job In Vague Terms

"Supporting the marketing team in promoting our products" is too vague. What does that mean? What level of performance is considered poor, good or great? Watch out for "-ing" verb tenses, as they are often too vague. Instead, consider a more specific statement of the job, such as "To help our customers modernize their inventory management systems by increasing sales of existing customers by 20% per year through new product introduction." We would consider that an essential statement of the role's mission, which is a high-level but specific explanation of why the job exists.

Focusing Only On Actions, Not Results

Some leaders make the mistake of wording their expectations in terms of only actions, not results. "Contact at least 20 existing customers per week and conduct an account review with at least five customers weekly." That is a perfect expectation of an "input" or an "action," but it is insufficient if all expectations are just actions, with no eye for the expected results. The risk is that people go through the motions of doing prescribed actions without feeling the urge to deliver a specific outcome. And your organization succeeds or fails based on results in critical areas, not actions.

Solely Focusing On Results, Not Actions

Other leaders make the mistake of wording their expectations in terms of big-picture results without regard to the actions that are likely to achieve them. "Grow revenue at least 15% per year" is a very specific "what." But to make that expectation more achievable, you must also list several actions that are expected to help achieve that result.

Instead of creating job descriptions, I encourage colleagues and clients to follow a practice called writing a "scorecard." A scorecard has a clear mission for the role. It identifies 5–7 outcomes you expect a person to achieve by a specific date. The outcomes are a mixture of actions you want the person to take and the results you expect them to achieve. This makes it easy to "score" whether someone has achieved the outcomes. Using a scorecard will improve your ability as a leader to hire and coach people to embody the organization's purpose and take actions that achieve results.

Dr. Geoff Smart is chairman & founder of ghSMART, a leadership consulting firm that exists to help leaders amplify their positive impact on the world. Dr. Smart and his firm have published multiple New York Times best sellers. He stays active in his community and has advised many government officials.

IS IT TIME TO DITCH THE PASSWORDS FOR MORE SECURE PASSKEYS?

Passwords are the most used method of authentication, but they are also one of the weakest. Passwords are often easy to guess or steal. Also, many people use the same password across several accounts. This makes them vulnerable to cyber-attacks.

The sheer volume of passwords that people need to remember is large. This leads to habits that make it easier for criminals to breach passwords. Such as creating weak passwords and storing passwords in a non-secure way.

61% of all data breaches involve stolen or hacked login credentials.

In recent years a better solution has emerged – passkeys. Passkeys are more secure than passwords. They also provide a more convenient way of logging into your accounts.

What is Passkey Authentication?

Passkeys work by generating a unique code for each login attempt. This code is then validated by the server. This code is created using a combination of information about the user and the device they are using to log in.

You can think of passkeys as a digital credential. A passkey allows someone to authenticate in a web service or a cloud-based account. There is no need to enter a username and password.

This authentication technology leverages Web Authentication (WebAuthn).

This is a core component of FIDO2, an authentication protocol. Instead of using a unique password, it uses public-key cryptography for user verification.

The user's device stores the authentication key. This can be a computer, mobile device, or security key device. It is then used by sites that have passkeys enabled to log the user in.

Advantages of Using Passkeys Instead of Passwords

More Secure

One advantage of passkeys is that they are more secure than passwords. Passkeys are more difficult to hack. This is true especially if the key generates from a combination of biometric and device data.

Biometric data can include things like facial recognition or fingerprint scans. Device information can include things like the device's MAC address or location. This makes it much harder for hackers to gain access to your accounts.

More Convenient

Another advantage of passkeys over passwords is that they are more con-

venient. With password authentication, users often must remember many complex passwords. This can be difficult and time-consuming.

Forgetting passwords is common and doing a reset can slow an employee down. Each time a person has to reset their password, it takes an average of three minutes and 46 seconds.

Passkeys erase this problem by providing a single code. You can use that same code across all your accounts. This makes it much easier to log in to your accounts. It also reduces the likelihood of forgetting or misplacing your password.

Phishing-Resistant

Credential phishing scams are prevalent. Scammers send emails that tell a user something is wrong with their account. They click on a link that takes them to a disguised login page created to steal their username and password.

When a user is authenticating with a passkey instead, this won't work on them. Even if a hacker had a user's password, it wouldn't matter. They would need the device passkey authentication to breach the account.

"New vulnerabilities are discovered every day, so even if no changes are deployed to your systems, they could become vulnerable overnight."
The Hacker News

Enable 24/7 scanning to be on top of your IT security