TECH SOURCE

November 2018

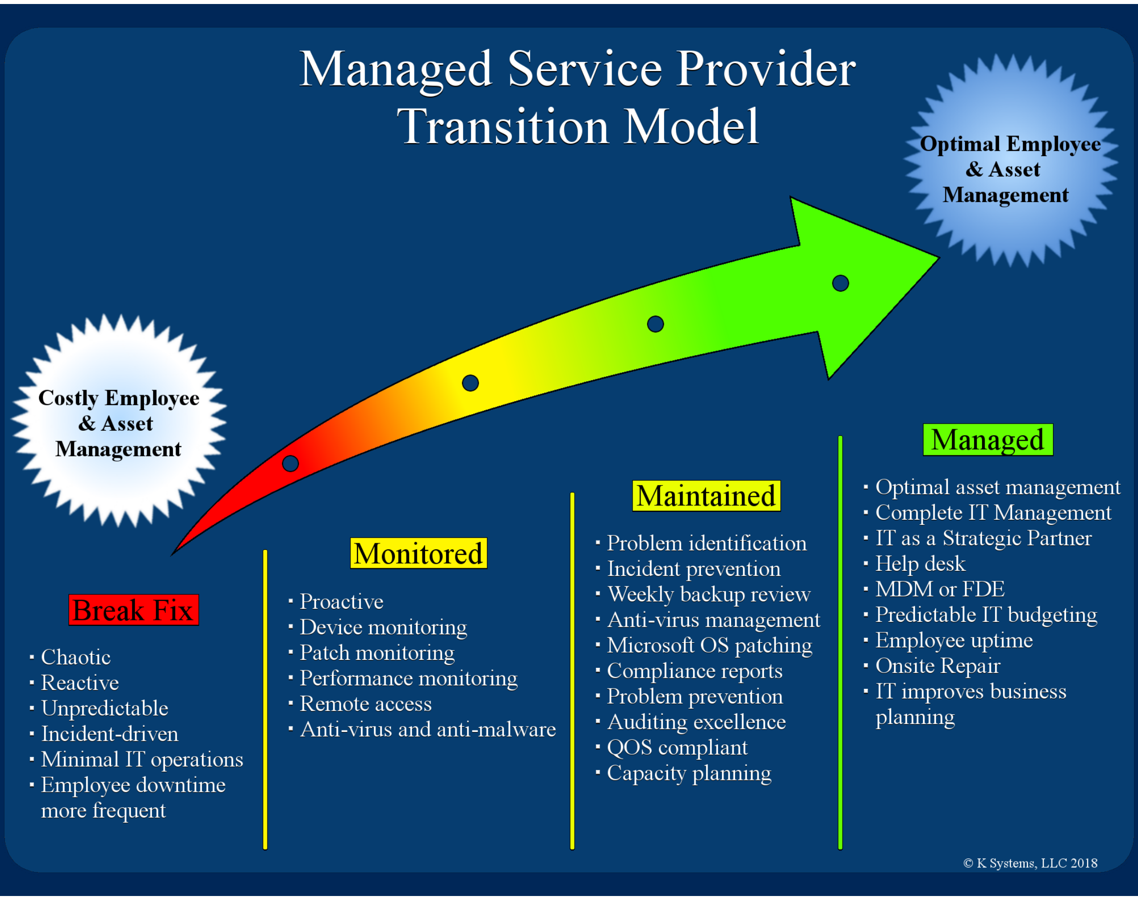
Volume 1 - Why use a Managed Service Provider

Phone: 504-888-8324

Visit us at: 888-tech.com

What is a Managed Service Provider?

As a Managed Service Provider (MSP), we are your personal IT department. You do what you do best and let us keep up with the ongoing technological landscape and its always-changing arena. We can guide you through the reactive/break-fix environment to a proactive, managed and monitored atmosphere where we see problems before they occur. This helps us limit downtime and inefficiencies as well as achieve optimal employee and asset management.



Managed Service Provider Transition Model

Optimal Employee & Asset Management

Costly Employee & Asset Management

Break Fix

- Chaotic
- Reactive
- Unpredictable
- Incident-driven
- Minimal IT operations
- Employee downtime more frequent

Monitored

- Proactive
- Device monitoring
- Patch monitoring
- Performance monitoring
- Remote access
- Anti-virus and anti-malware

Maintained

- Problem identification
- Incident prevention
- Weekly backup review
- Anti-virus management
- Microsoft OS patching
- Compliance reports
- Problem prevention
- Auditing excellence
- QOS compliant
- Capacity planning

Managed

- Optimal asset management
- Complete IT Management
- IT as a Strategic Partner
- Help desk
- MDM or FDE
- Predictable IT budgeting
- Employee uptime
- Onsite Repair
- IT improves business planning

Why use a Managed Service Provider?

- Do you have a cost effective solution?
  - ***Per glassdoor.com, the average on staff, IT labor resource is $50,000-60,000 a year ($5,000 per month) compared to our MSP services at about $65 per computer per month.***
- Do you have a back up system in place?
  - ***With our Maintained Service Level, we provide cloud and local backup solutions which we check weekly.***
- Do you need a secure way to share files inside or outside the company?
  - ***With our Maintained Service Level, we provide a secure cloud and email file sharing tool.***

Benefits of an MSP:

- Keeps you focused on your business while we focus on the technology
- Gives you access to the latest technologies
- Can provide a disaster recovery plan for computers and servers
- Allows us to provide layers of security

Click here if you would like to learn more about our services

Hot Topic of the Month - Cybersecurity

As National Cybersecurity Awareness Month ends, it's important to understand what cybersecurity is and how you can ensure your internet connected devices are safe.

What is Cybersecurity?
Cybersecurity is the protection of any systems (software and hardware) connected to the internet. With constant evolving technology, security is changing. It is important to keep up with new security practices so your systems can remain safe from cyber attacks.

Cybersecurity is the responsibility of governments, companies, groups, and individuals to protect themselves from malicious cyber content. *You are responsible for keeping your data and devices safe*.

The Department of Homeland Security's online safety tips:

- **Enable stronger authentication.** This provides an extra layer of protection by verifying the user who is logging in. Most major social media, financial, and email accounts allow you to add a stronger authentication method, such as two-step or multi-factor authentication.
- **Make your passwords long & strong.** Create passwords that use numbers, symbols, and letters. Remember to change your passwords regularly, as well as use unique passwords for different accounts.
- **Keep a clean machine.** Focus on keeping your security software, operating system, and web browser up to date. We offer this service as part of our maintained service level.
- **When in doubt, throw it out.** Links in email and online posts are often the way cyber criminals compromise your computer. If it looks suspicious, delete it.
- **Share with care.** Limit the amount of personal information you share online and use privacy settings to avoid sharing information widely. We offer Security Awareness Training (SAT).
- **Secure your Wi-Fi network.** Cyber-criminal's primary source of entry to your network is through your wireless router. Make sure you change your router's username and password from the factory default.

US-CERT tips to protect yourself from malicious code | **Read other tips from US-CERT**

If you found this newsletter helpful, feel free to forward it.

Register for Newsletter

Visit our website