directive

TECHMinutes

January 2020

Your Small Business Technology Information Source!

This Issue:

How a Co-Managed Strategy Can Be a Game Changer

Your Business Will Benefit from Proper Data Management

Is Your Business in Need of Managed IT?

The End for Windows Server 2008 and Windows 7 Just Days Away

Baseline Cybersecurity

Smartphone Malware Is a Serious Threat

Is Your Business in Need of Managed IT?

Technology is outrageously helpful in many aspects of life, especially modern business practices. Of course, this is assuming that this technology is in proper working order for most of the time. In order for enough productive work to take place within an organization, the team must be sure **the tools they need for this work are ready for them to do so.**

However, this is often easier said than done.

As businesses have adopted more and more technology, their work-essential tools have grown more complicated while they have grown more sufficient, which means that properly...

Read the Rest Online!
https://dti.io/inneed

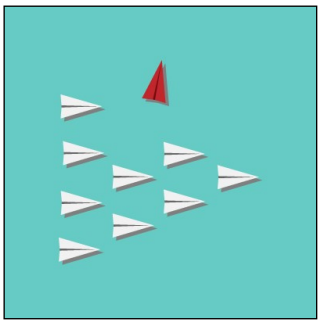
About Directive

We are a technology consulting firm specializing in technology implementation and management for businesses. We're known for providing big-business, Enterprise-Level IT services to small and medium-sized businesses.

Visit us **online** at:
newsletter.directive.com

It has been our honor to have been your trusted provider in 2019. Our New Year's resolution is to make 2020 even better - and this one will last longer than resolutions usually do!

How a Co-Managed Strategy Can Be a Game Changer



We always try to communicate the numerous benefits of managed IT services, but when your business is happy to have their own internal IT department, those benefits tend to look less appealing. For organizations that rely on the expertise of their internal IT staff, they may not think they have a need for --or simply can't afford--an outside IT presence. This misconception may actually be harming their businesses. Today, we will introduce co-managed IT services, and how they can be leveraged to maximum benefit.

Most companies choose to utilize either a dedicated IT department or outsource their technology to a provider that manages, monitors, and maintains the network and infrastructure (mostly) remotely. There are benefits to both methods, but sometimes one method isn't enough. The IT department can be stretched too thin. It can either be distracted with new

(Continued on page 3)

Your Business Will Benefit from Proper Data Management

As digital systems have been adopted by more businesses, data has become a bigger tool. This is due to businesses having the initiative to direct this data into creating strategy. Today, data services are a desirable component for a business to embrace. Let's take a closer look at how businesses are expanding their use of their data.

First, we need to specify what we mean when we reference "data services."

You may have heard the term "big data" before. Once exclusively available to large companies, this term is the shorthand for the collection and analysis of all kinds of data. As the technology has improved and become more affordable for small businesses to adopt, more of these small businesses are using it to their operational benefit.

Therefore, when we use the term "data services," we're talking about the services that rely on this data to function optimally, initiatives like business intelligence, analytics, and backup and disaster recovery. Each serve a different role within a business, but if a business makes use of each, they will deliver significant value. Let's consider how each can (and should) make use of data.

(Continued on page 2)

The End for Windows Server 2008 and Windows 7 Just Days Away

Microsoft is just days away from officially retiring their Windows 7 and Windows Server 2008 R2 operating systems. If your business is, for whatever reason, still using this software, you will need to upgrade by January 14 or face using unsupported software that could quickly become a security problem for your business. Let's take a look at your options.

Option #1 - Purchase New Hardware and Migrate Your Data

The first option is the most expensive; and, since there isn't a lot of time to make this move, it will cost even more to upgrade today than it would have months (or years) ago. The professional consultants at Directive can move fast to migrate your data over to new servers and workstations that run supported software, but since IT projects typically move slowly, waiting to the last minute is sure to have consequences. Your Windows Server 2008 R2 servers and your Windows 7 workstation will still work, but finding the right hardware, OS titles, and compatible software to keep your business from being hindered by the multitude of problems that running your business on unsupported software is bound to present, is critical.

To save some money if this is the route you are considering, some of your existing hardware may be able to run Windows 10. Here are the bare minimum specifications that are required to run Windows 10:

- **Processor -** 1 GHZ or faster
- **RAM -** 1 GB for 32-bit or 2 GB for 64-bit
- **Hard disk space -** 16 GB for 32-bit or 20 GB for 64-bit
- **Graphics card -** DirectX 9 or later with WDDM 1.0 driver
- **Display -** 800 x 600 resolution

This is the absolute minimum so don't expect Windows 10 to zip around if these are the specs on the workstation. We recommend at the very least some type of 2 GHz dual-core processor, 4-to-8 GB of RAM, and at least a 160 GB hard drive.

Option #2 - Virtualize

Another option your business has is to migrate your data over to the cloud. Today's virtualized environments are often much more cost effective than the purchase of new hardware. You can host servers of all types. Today, organizations are using virtual machines in AWS and Microsoft Azure to deliver cost-effective solutions running Windows 10, as well as any other software the business depends on.

Some of the benefits of virtualization include an initial cost reduction as there are no large purchases to be made. You'll likely need to purchase some low-end thin clients, since you won't want your users remoting in on outdated...

Read the Rest Online!
https://dti.io/theend

Your Business Will Benefit from Proper Data Management

(Continued from page 1)

Backup and Disaster Recovery (BDR) Solutions

If you're using data to your advantage, you need to be sure that the data you are using is protected--the same goes for data that you aren't currently using as well, as you never know when it might come in handy. A BDR platform ensures that--by backing up the data you specify - your important data and resources can be recovered after a disaster event influences them. More than that, regardless of the reason recovery in necessary (natural disaster, malware infection, or good, old-fashioned human error) a BDR can help make it more likely that the files you can recover are relatively recent and up-to-date.

A BDR is a network-attached device that saves backups of your data incrementally. For complete protection, your data is also pushed to an offsite secure location, insulating your data from the impact of a disaster upon your business. While a BDR can be purchased on its own, it is also a common component of a managed service agreement.

Business Intelligence

Business intelligence is the term for taking collected data and using it to make decisions that best maintain and streamline an organization's operations. Using reports and other visual interpretations of data, BI is intended to improve business efficiency and productivity. Data is summarized to give insights into different parts of a business, determining how they have functioned, and why.

Using BI can help to identify where a business is strong (and where it isn't) by analyzing financial and operational statistics, assisting decision makers support their choices through empirical data, rather than just their gut. With the bird's-eye view that BI can deliver, it is much simpler to develop practicable goals and actionable game plans.

Business Analytics

Business analytics, or BA, are somewhat similar to the use of business intelligence, as both use data analysis to differences in that BI focuses on past patterns and their current outcomes, rather than trying to predict the best course to follow for the future, as business analytics does.

To learn more about how you can make the most use of your business' data, while protecting it and your other assets, reach out to the IT professionals at Directive. Start a conversation by calling 607.433.2200.

Share this Article!
https://dti.io/proper

How a Co-Managed Strategy Can Be a Game Changer

(Continued from page 1)
technology projects and lapse on the comprehensive management and maintenance of the organization's IT; or, it can be forced to deal with all the technology problems that it doesn't have time for the research and effort new projects often command. This leaves the organization short on coverage and on options.

On the other hand, an MSP may use all the tools and expertise to properly manage and maintain the technology, but much of their expertise is delivered remotely. As a result, some businesses will spend more money hiring a dedicated team because they know where these professionals will be and can ensure that problems are handled immediately.

This is Where Co-Managed IT Comes In

The co-management of an organization's IT starts with the onsite IT administrator, or team of technicians. On average, IT professionals command around $63,000 per year. That means it may not be financially viable to pay the amount of technicians needed for coverage. Since they would typically be asked to look after all the technology for the company, having a shortage in talent can be a real problem.

Many organizations that are looking to add productivity-fueling technology to their business take a long time to implement solutions. Co-management adds flexibility to your IT department by contracting a managed services provider to fill in the gaps. It frees the in-house IT staff up to focus on strategic IT issues by delivering comprehensive IT support...

Read the Rest Online!
https://dti.io/comanage

Baseline Cybersecurity

More than any time before, cybersecurity has to be a major consideration for businesses. It is, in fact, one of the biggest problems the modern business has to face day-in and day-out. Shortage in cybersecurity talent and antiquated strategies are making it difficult for businesses to find the knowledgeable resources that will help them work to secure their network and data from threats to the business.

Cybersecurity is in large part eliminating risk. Today, we share five tips that will go a long way toward helping a business understand where the threats come from. Of course, these aren't ironclad policies enacted to protect data. They are simply tips designed to help an organization better manage their computing resources from cybercriminals:

#1 - Keep a Clear Inventory of Assets

What do you need to protect? Everything? Then you need to inventory everything. This includes every wire, extra peripheral, and piece of software your business has purchased. By knowing exactly what hardware and software you possess, the easier it will be to manage it.

#2 - Educate Users on Cybersecurity Best Practices

By training your staff on the best practices needed to secure your business' computing network, you are giving them more than just a security lesson. We like to call it cyber hygiene. Since their cyber behavior matters, the more they know about how to spot phishing attacks, how to create and use proper passwords, and how to build work profiles on their mobile devices, the stronger your organization's security efforts are.

#3 - Address the Shadow IT Problem

Shadow IT may not be at the top of the list of priorities. Some people won't be familiar with the term. It is software that is downloaded by end users that hasn't been approved by an organization's IT administrator. In order to keep software from being vulnerable it has to actively be patched with security updates. If end-users are just downloading any program they want, what's stopping an infected program from appearing on your business' network one day? Nothing. Make sure your staff has a clear understanding of what software is allowed and how to download and update approved software titles.

#4 - Have Tools In Place

Comprehensive cybersecurity is dependent on sticking to solid practices, understanding the threats, and having the tools in place to ensure that security can be maintained. Tools such as antivirus and anti-malware, content filtering, spam blocking, and a strong, constantly updated firewall go a long way toward giving any organization a shot at keeping threats from becoming a huge problem for a business.

#5 - Sometimes IT Gets Old

Traditionally, the older a piece of technology gets, the less effective it is. Having a strategy of upgrading away from old technology, and keeping your technology patched and updated, your company will have the best chance of protecting your business' digital assets and keeping malware, hackers, and the like out of your network.

Do you need technology tools and services to keep your business safe? Our professional technicians can help you with many facets of your cybersecurity policy. Call Directive at 607.433.2200 today.

Share this Article!
https://dti.io/techtools

Smartphone Malware Is a Serious Threat

We all know how important it is to protect your desktop and laptop computers from malicious threats. Installing antivirus and security software is one of the first steps you take when you get a new computer, and for good reason. An unprotected device is at great risk. With that said, a lot of users don't think about the threats that target their most-used devices, their smartphones.

Malware and other cybersecurity threats are not a new thing to smartphones and mobile devices, but they don't tend to get the same attention as threats that target Windows. This might be because, for the most part, mobile device malware is a little less common, or at least a little less intrusive. That doesn't make it any less of a problem though.

You might also feel a little less at risk simply because of your relationship with your device. Our smartphone is often with us day and night, at work and at home. Combine that with the fact that most users use their smartphones in a sort of echochamber, they might not be directly exposed to threats as often as they are on a PC. We'll get to more on this shortly, but first it's important to break down the risks based on whether you have an iOS or Android device.

iPhone Malware

Apple may tout iOS as being the safest mobile operating system on the market, but it has never been completely safe. The biggest risks are only a problem for users who have jailbroken iPhones, meaning they 'hacked' their own device to allow themselves to bypass Apple's built-in security restrictions. If you haven't done that, you are avoiding a lot of risk. The other risk, which is less common, involves a more major type of risk called a zero-day hack. **Zero-day** hacks target devices that haven't received a security update after the security update has been released to the public.

The problem with iOS security is that there aren't a lot of ways to prevent the issue, and you are really at the mercy of Apple to keep your device safe. They certainly want to keep their reputation, so trusting in them to do so isn't invalidated.

Android Malware

Android is in a different situation. There are a lot more risks for Android devices, simply because there are many different manufacturers making and supporting the operating system. For example, Samsung uses a slightly customized version of Android, and if you have a Galaxy Note 10, you'll get the latest updates to Android on a different schedule than Google's Pixel.

Android is also more open and flexible than iOS, which is why a lot of users prefer Android over iOS. If you want to install an application that hasn't been vetted by Google, you can. You can also jailbreak an Android device, which, similar to jailbreaking an iPhone, can override some of the built-in security restrictions.

Even installing apps off of the Google Play Store can sometimes lead to malware being installed. Google has had to play cat-and-mouse with app developers to keep threats off the marketplace, but it has become clear that it really comes down to the user being careful with what they install.

That isn't to say you should abandon Android or restrict your employees from using Android devices to access company email or other apps. Many long-time Android users never experience malware - it depends on how you use your device.

How to Protect Your Smartphone from Malware

Rely on that Echochamber - We mentioned this earlier, but both Android and iOS feature their own app stores. Although Android devices can install applications that aren't on the Google Play store, most modern...

Read the Rest Online!
https://dti.io/phonethreat

We partner with many types of businesses in the area, and strive to eliminate IT issues before they cause expensive downtime, so you can continue to drive your business forward. Our dedicated staff loves seeing our clients succeed. Your success is our success, and as you grow, we grow.

Chris Chase
Solutions Integrator

Charlotte Chase
Solutions Integrator

Directive

330 Pony Farm Road
Suite #3
Oneonta, NY 13820
Toll-Free 888-546-4384
Voice: 607-433-2200

Visit us **online** at:
newsletter.directive.com

newsletter@directive.com
facebook.directive.com
linkedin.directive.com
twitter.directive.com
blog.directive.com
instagram.directive.com