Tech Solutions INC.
Managed Services
Computer Consulting
Network Administration

TechPoints

July 2014 | *IT Tips and TechSolutions News* | Vol. 4 No. 7

In This Months TechPoints

- 4 Great Tips for BYOD Security
- Continuity Metrics: RTO and RPO
- 5 iPhone Messaging Tips
- 10 Important Virtualization Terms

4 Great Tips for BYOD Security

BYOD, or Bring Your Own Device, is one of the most common business trends of the past couple of years. To many, the idea of bringing their own phone, tablet, laptop, or even computer to the office is ideal because it is a system they are undoubtedly familiar with. They may also view personal devices as better than the office models. Even if you don't allow your employees to bring their own devices to work, there is a good chance they do anyways. However, this could pose a security risk that needs to be dealt with.

What should I do about BYOD?

The first reaction of many office managers and business owners, worried about security threats that could stem from BYOD, is to impose an outright ban of devices. While telling your staff they are not to use their devices for work may seem like a quick and easy solution, you can be 100% sure that there will be employees who ignore this policy and use their personal devices for work regardless.

This could put your business at a higher security risk if the rule is ignored, especially if you don't implement any security measures to protect your networks and data. In order to minimize the potential threats BYOD can expose your business too, we suggest you do the following:

1. Consider embracing BYOD

Instead of simply banning personal devices in the workplace take a step back and look to see if there are any benefits BYOD can offer. For example, if you operate on razor thin margins and have not replaced hardware in years, there is a good chance your employees will have better systems at hand. This could help you reduce your overall tech costs.

The same goes for phones for your employees. Why not offer to pay for the plan and allow employees to use their own devices? Of course, you are going to want to implement security measures and usage rules, but if this is easily achieved then it may help reduce your overall operating costs. Before you do implement a system like this however, we strongly recommend you read the rest of this article and follow the steps below.

2. Set up separate networks for employee devices

Oftentimes, the main reason employees bring their devices to the office and use them for work purposes, especially when it comes to mobile phones, is because they can happily connect to Wi-Fi for free without using their data plans throughout the day.

Chances are high that because they use the work Wi-Fi on their device for non-work tasks, they simply keep using the device when they are doing work related activities. This could pose a security risk, especially if you run business-critical operations on the same network. You could nip this potential problem in the bud and simply install another Wi-Fi network for mobile devices and non-critical business processes.

It is usually quite affordable to simply purchase another line and the networking equipment to support this, not to mention the fact that it will keep business-critical processes secure from errant malware. As an added bonus, you will likely see increased productivity because the bandwidth demand will be limited, so important data will move quicker.

3. Educate your staff about security

In our experience, the vast majority of BYOD related security risks are exposed by mistake. An employee may have a virus on a personal phone and be unaware of it. When they connect to the network it can then be unintentionally spread to other computers resulting in a potentially massive security breach.

One of the simplest ways to prevent this is to educate your employees about proper mobile safety. This includes how to spot apps that could contain malware, sharing security threat updates, and teaching your employees how to secure their devices. You really need to stress just how important security is to them.

On top of this, contact an IT expert like us for a recommended anti-virus and spyware scanner for mobile devices that users can easily install. Encourage employees to not just install this but to keep it up to date too. Many of these mobile specific scanners are free and just as powerful as desktop versions.

4. Work with an IT partner to establish a solution that works for you

Beyond education and simple network establishment, it is a great idea to work with an IT partner like us. As experts, we keep tabs on the trends and solutions related to BYOD and will work with you to establish a program that works for your company.

It may be that you don't actually need to integrate BYOD but to update hardware or software to newer versions instead. It could be that there is a simple solution to employees feeling frustrated with slow performance of existing systems at work.

If you do implement BYOD, we can help establish security measures and policies that will ensure your networks and employee devices are secure. The best advice we can give however, is to do this before you start allowing BYOD, as it can be far more challenging to implement and enforce changes when employees are already using their devices at work.

Published with permission from TechAdvisory.org

Continuity Metrics: RTO and RPO

When it comes to ensuring that your business will not only recover from the next disaster, but also be able to continue to operate, it is essential that you implement a business continuity plan (BCP). When developing and fine-tuning these plans there are a number of key metrics you should be aware of, with the two most important being RTO and RPO.

While both RTO and RPO are important elements of continuity plans, and they both sound fairly similar, they are actually quite different. In this article we define RTO and RPO and take a look at what the difference is between the two concepts.

RTO defined

RTO, or Recovery Time Objective, is the target time you set for the recovery of your IT and business activities after a disaster has struck. The goal here is to calculate how quickly you need to recover, which can then dictate the type or preparations you need to implement and the overall budget you should assign to business continuity.

If, for example, you find that your RTO is five hours, meaning your business can survive with systems down for this amount of time, then you will need to ensure a high level of preparation and a higher budget to ensure that systems can be recovered quickly. On the other hand, if the RTO is two weeks, then you can probably budget less and invest in less advanced solutions.

RPO defined

RPO, or Recovery Point Objective, is focused on data and your company's loss tolerance in relation to your data. RPO is determined by looking at the time between data backups and the amount of data that could be lost in between backups.

As part of business continuity planning, you need to figure out how long you can afford to operate without that data before the business suffers. A good example of setting an RPO is to imaging that you are writing an important, yet lengthy, report. Think to yourself that eventually your computer will crash and the content written after your last save will be lost. How much time can you tolerate having to try to recover, or rewrite that missing content?

That time becomes your RPO, and should become the indicator of how often you back your data up, or in this case save your work. If you find that your business can survive three to four days in between backups, then the RPO would be three days (the shortest time between backups).

What's the main difference between RTO and RPO?

The major difference between these two metrics is their purpose. The RTO is usually large scale, and looks at your whole business and systems involved. RPO focuses just on data and your company's overall resilience to the loss of it.

While they may be different, you should consider both metrics when looking to develop an effective BCP. If you are looking to improve or even set your RTO and RPO, contact us today to see how our business continuity systems and solutions can help.

Published with permission from TechAdvisory.org

---

5 iPhone Messaging Tips

The days of simple texting are behind us. Today, messaging apps like the iPhone's Messages allow you to do much more than sending a block of text. With business operators relying on messaging apps more than ever before, let's take a look at five iPhone messaging tips that will help make your communication experience a little easier and faster.

1. Create Shortcuts

Have you ever typed phrases that you often use on the iPhone messaging app only to correct the typos that often come from typing on the touchscreen? To do away with this annoyance, you can create shortcuts for phrases by going to Settings>General>Keyboard>Shortcut and clicking on Add new shortcut. Now, whenever you type in a particular word that matches the shortcut you've entered, you won't have to type out that entire phrase again.

2. Voice Messages

While voice messages have been ignored by many people, they're actually a fast and effective way to communicate in the iOS messaging app. Simply record any message through the Voice Memo that is available in the Utility folder and tap on the arrow symbol in your recording page to share them on your messaging app. Now you won't have to worry about typing your message or there being any sort of miscommunication again.

3. Share Contacts

Sharing contacts is handy for business operators. And while you'd usually go into your contact page and type in a contact's phone number, there is a quicker way to get the job done. Simply tap into contact information and then scroll down and hit the Share Contact option. Not only will you eliminate having to type that contact's phone number, but other information from that contact such as their email or work address will also be shared without you having to copy and paste it.

4. Share Messages

Sharing of information is a basic task in any business, and if you want to share a message but don't want to type it out or even copy and paste it, the iPhone messaging app features another alternative. All you have to do is tap and hold down the message, tap on More and then on the blue arrow on the bottom right corner of the prompt command. By doing this, your message will be placed in a new message screen and you can simply choose your recipient.

5. Hide Message

We all need some privacy, especially where work is concerned, and the messaging app on the iPhone allows you to keep your messages to yourself by stopping the message preview from showing in the Notification Center. Go to Settings>Notification Center >Messages, then tap Show Preview to turn the message preview off. Now, when you receive a message, your iPhone will only display who sent that message without compromising its content.

Familiarizing yourself with iPhone's messaging capabilities will save you time and frustration – and in chaotic business environments that can be a huge advantage.

Published with permission from TechAdvisory.org

10 Important Virtualization Terms

Virtualization – the act of moving something physical to a digital environment, normally delivered over a network connection – is one of the most beneficial tech concepts, especially for small businesses. For many business owners and managers however, this is a vastly complex concept, that carries with it some confusing terminology. To help, we have come up with a glossary of 10 virtualization terms every owner, manager, and employee should be aware of.

1. Virtual Machine (VM)

You will often hear virtualization experts bandy about the term VM. What they are talking about when they say this is the Virtual Machine. The VM is essentially a virtual representation of the computer on your desk. It can do everything a physical machine does, only everything is virtual and usually delivered over a network connection. Because VMs are software based, you can often run more than one VM on the same physical machine. This could equate to having say two separate versions of Windows running at the same time, or even running a different operating system, say Windows on your MacBook.

2. Virtual server

A specific type of VM, in this case a server, that is running in a virtual environment. A common setup many offices employ is to have one physical server on premise. This server then hosts separate virtual servers that in turn host different services like email, networking, storage, etc. Other businesses choose to rely completely on virtual servers. This is where another company hosts the servers which are delivered to you over the Internet. To the computers and users it appears the servers are there on your network, and can be interacted with normally when in truth, the servers are actually virtual.

3. Virtual desktop

Much like the virtual server, the virtual desktop is a specific type of VM. In this case, it is a virtually delivered version of an operating system like Windows, Linux or even OS X. Since the advent of virtual desktops, the idea that companies have to stick with one type of operating system has started to become irrelevant. For example, if you own a Mac and need to access a Windows only program, one solution is to use a virtual version of Windows. If you have access to one, you will be able to run Windows from your Mac without having to physically install it on your computer.

4. Hypervisor

The hypervisor is essentially a small operating system that enables virtualization. Its job is to take physical hardware resources and combine them into a platform that is then delivered virtually to one, or many different users.

5. Host system

The host system, also referred to as the parent, is where the physical hardware and software is installed. These physical components are then copied by the hypervisor and delivered in a virtual state to the user. If you are creating a virtual desktop environment, then the host system will have the desktop's OS installed on it, along with the necessary software.

6. Guest system

The guest system, also referred to as the child, is where the VM is accessed. To carry the example on from above, the OS that is installed on the host machine is replicated by the hypervisor and the copy is then delivered to the user. The user can interact with the OS just as they would with the physical host machine, because the guest system is an exact copy of the host. The only difference is, the guest machine is virtual instead of physical.

7. Virtual Infrastructure

When you combine a bunch of different types of VMs together into one solution, including hardware, storage, desktops, and servers you create a virtual infrastructure.
This can then be deployed to businesses who are looking for a completely virtualized solution. The easiest way to think of this is that your whole IT infrastructure is combined into one solution and virtualized. Many companies look for a solution like this because it reduces the need for on-premise hardware, while making it easier for an IT partner to manage.

8. P2V

P2V, or Physical to Virtual, is a term used by IT experts to refer to the act of migrating a physical system to a virtual one. The most common example of P2V is the merging of physical servers into a virtual environment that is hosted on one server.

9. Snapshot

A snapshot is an image of the state of the virtual machine at a specific point of time. This includes all of the data, configurations, and even windows or programs open at that time. Snapshots are used kind of like the Save button on video games – it saves your progress. When you next load up the VM, you will get all of your data, programs, and configurations back. Snapshots are also kept in case something goes

wrong with the VM. You can easily revert back to an older snapshot, one that was taken before the problem.

10. Clone

The action of taking one VM and creating an exact copy that can then be used by another computer or user.

If you are looking to learn more about virtualization, contact us today to see how we can help.

Published with permission from TechAdvisory.org.

TechPoints is a monthly newsletter from TechSolutions, Inc.

Click here to unsubscribe and simply put "Unsubscribe" in the subject line.

TechSolutions, Inc. ● 5630 Kirkwood Highway, Wilmington, DE 19808 ● www.TechSolutionsInc.com ● (302) 656-8324