GLOBALTECH SOLUTIONS

This Issue:

Tips to Help Manage your IT Inventory Better

IT inventory management, also known as IT asset management or ITAM, is an important process for any business to undergo. This is effectively the process of ensuring that all of your information technology resources are accounted for and protected. Here, we've assembled some practices that will help make this process much simpler.

First, let's delve into what ITAM actually covers.

Understanding ITAM

Consider all of the internal resources that your business uses...

Read the Rest Online!
http://bit.ly/2LiGWeX

About Global Tech Solutions

We provide IT Support such as technical helpdesk support, computer support, and consulting to businesses nationwide. It's always been our goal to provide enterprise-level IT practices and solutions, with small business prices.

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

Happy New Year!

We are happy to have had the opportunity to work with our clients for this past year. Here's to another year of successes, prosperity, and good fortune!

Networking Isn't What It Used to Be

There are times when people take their technology for granted. One of the most under-the-radar, yet crucial parts of a business' technology infrastructure is the networking equipment. What we mean by this is the cables, switches, and routers that connect computers to the network and to the Internet. This month, we will take a look at typical office networking found in 2019 and the technologies that are primed to replace them.

Connecting Your Office

The modern office functions a lot like the office of twenty years ago in terms of networking. Most of the time, endpoints connect to switches that connect to routers that connects to servers and the internet. This has been the way it has been for a couple of decades. Sure, the technology itself has been improved drastically, bandwidth dwarfs older connection speed, but all-in-all it is pretty similar to the way that office networking has been structured for some time.

One major change is the reliance on Wi-Fi. Wireless internet provides a more flexible work environment, giving staff a better ability to collaborate through the use of mobile devices

Five Steps to Better Basic Cybersecurity

Cybersecurity needs to be one of any business' primary considerations. More than it ever has been before, cybersecurity is one of the biggest day-to-day issues that a business needs to deal with; and, this need is only exacerbated by the shortage of cybersecurity talent and loyalty to outdated security strategies have put many businesses in an unenviable, and vulnerable, position.

One crucial component of any successful cybersecurity practices is the active effort to eliminate risk wherever possible. Here, we've compiled five practices that will contribute to your business' capability to recognize where its threats come from. While these aren't exactly policies to help protect your data, they can help you collect the data you need to form these policies.

1. Inventory All of Your Assets

When you resolve to protect everything, as many business owners do, it helps to know what exactly "everything" includes. Maintaining a comprehensive inventory of all of your technology-- each wire, additional peripheral, and software title your business has acquired--makes managing your technology far simpler and more efficient.

The Latest Android Malware is Almost Impossible to Remove

Sometimes a virus or malware infection can be so bad that the best solution is to completely wipe the device and start over with a factory reset. This can be pretty annoying. A new type of malware targeting Android devices just found a way to become even more annoying by being able to withstand a complete factory reset.

Meet xHelper, the Malware That Refuses to Go Away

As of right now, it is suspected that xHelper has infected around 50,000 devices, which is a big number, but relatively low when it comes to malware of this type. The big names in cybersecurity, Symantec, Malwarebytes, and the like, don't have any clear answers on how to actually remove the threat. If that's not enough, deleting everything on your smartphone and doing a factory-reset won't remove the malware

either. Once you set your device back up, the threat will be back.

What Does xHelper Do?

We have good news and some bad news. The good news is that right now, it seems that xHelper just gives you annoying pop-up spam and notifications. It's goal? To get you to install more applications, and likely these applications could come with additional threats.

It is also suspected that xHelper can download and install apps on its own. It hasn't been officially detected doing this in the wild yet, but if it could do that, then you would essentially lose control over your device.

Don't Forget, You Can't Get Rid of xHelper Once You Get It

As of right now, there is no way to uninstall xHelper, and even resetting your device to factory settings keeps the malware installed. There is essentially no help for you other than getting a new phone, or waiting for Google or one of the major players in

cybersecurity to figure out a way to remove it. This could take a while...

For Now, All You Can Do is Avoid Getting xHelper

The malware seems to get installed from scammy websites. The app isn't found on the Google Play Store (at least at the time of writing this). Only install apps from the Google Play Store, and never from any other website. Google has a vetting process that keeps most apps on the Google Play Store relatively safe (it's not a perfect system, but it does weed out most of the danger).

When it comes to cybersecurity, the best place to get started is being aware of the threats and employing safe habits. That, and ensuring that your business data is thoroughly protected. Don't wait for a problem to happen, give Global Tech Solutions a call at (800) 484-0195 today.

Share this Article!
http://bit.ly/2PhbPl9

Networking Isn't What It Used To Be

(Continued from page 1)
such as laptops and smartphones. The integration of wireless connections necessitates the integration of security infrastructure and policies that work to keep unauthorized entities off of the business' computing network.

What is Changing?

You can count on one hand the inventions that have had the type of impact that the Internet has had on modern society. It's no secret that there is a worldwide push for ubiquitous Internet access. This push will no-doubt be felt inside the offices of businesses big and small for years to come. There are new considerations coming to the forefront of networking technology. Some of which promise to change the way networking works. These include:

Improvements to Wi-Fi

Wi-Fi 6, or 802.11ax, upgrades the

current highest-speed Wi-Fi available, 802.11ac. It brings a substantial improvement in efficiency across all current Wi-Fi bands, including older frequencies, such as 2.4 GHz. The biggest improvement Wi-Fi 6 brings is it increases the density of devices that can co-exist in a single space, increasing the networking speed on all devices.

Additionally, Wi-Fi 6 will improve performance by supporting packet scheduling that will make for dramatic improvements in power utilization by mobile devices. This will improve the wireless experience for every user and will substantially improve the way the Internet of Things is leveraged in the workplace.

Improvements to Wireless Mobile Networks

If you haven't heard about 5G yet, you will. The fifth-generation wireless

network is going to be a game changer. Wireless carriers are beginning to roll out 5G slowly and manufacturers have balked at going all-in on building 5G devices, but soon 5G will be the predominant wireless Internet platform and it will change everything.

5G will bring improved speed and battery life to smartphones and expand high-speed Internet for home users.

For the business, 5G will have less of an impact, but it will have one. 5G fixed access will be a useful option as a WAN connection for organizations that have multiple branches. Additionally, as 5G rolls out, it will present more opportunities for organizations to leverage the Internet of Things in new and useful...

Read the Rest Online!
http://bit.ly/2LlzCz4

Five Steps to Better Basic Cybersecurity

2. Push Cybersecurity Best Practices

Your staff, being the ones with their hands on your business technology, need to be trained on how to maintain its security. As it happens, this training should transcend just security and cover their cyber hygiene as well. The more they know about how to better secure their use of your technology and identify threats and issues, the more secure your business will be.

3. Address Shadow IT Head-On

Shadow IT is an insidious problem that many don't even consider an issue. The phrase "shadow IT" basically serves as a blanket term for any software that an end user has downloaded without the knowledge and approval of the IT administrator. While there are many potential issues with shadow IT, the worst of them likely comes from the vulnerabilities that unapproved and unpatched software can bring into the network. By enforcing a policy of utilizing only the solutions that IT has vetted and approved, you can protect your business from one of the least expected threats there is: the employee who was just trying to do their job.

4. Ensure the Proper Tools are Implemented

Cybersecurity, on paper, isn't such a difficult process. The issues come from the fact that everyone involved needs to understand the threats facing them and why the practices and tools they are expected to utilize are so crucial to security. Unfortunately, if the reasoning behind using antivirus and anti-malware, firewalls, spam blocking and content filtering (among other security tools) is never addressed, their use is more likely to be taken for granted, and ultimately neglected. Not only should these tools be in place, there needs to be an organizational commitment to using them… otherwise, threats are more likely to be an issue.
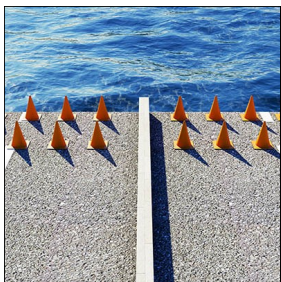
5. Keep IT Refreshed

As a general rule, the older your technology gets, the less effective it is at serving its intended purpose. This can…

Read the Rest Online!
http://bit.ly/2RgucJD

With Multiple Windows EOL Events, You Need to Have a Plan

January 14 marks the end of two Microsoft operating systems: Windows 7, and Windows Server 2008 R2. After these titles are retired, using them could quickly result in a major problem for your business' IT security. If you haven't made the switch to other solutions by now, you are running out of options. Let's quickly go over what you can do.

Upgrade Your Hardware and Migrate Over Your Data

Unfortunately, this option has two considerable downsides: it's going to be pretty darn expensive, and since there is a very limited amount of time to get it done, you'll likely have to pay even more to expedite the process. Furthermore, despite the professionalism and skill that our consultants at Global Tech Solutions will bring to the table, rushing this normally slow and controlled process is bound to create complications. Sure, Windows Server 2008 R2 and Windows 7 may still work, technically speaking, but it will only become harder to find the other components that play nicely with the software you rely on - not to mention riskier to even attempt.

Before you bite the bullet and replace all of your hardware, you may have the option to simply upgrade the solutions present in your infrastructure already. Windows 10 has a few fairly attainable benchmarks. They include:

- **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

Having said that, these are the minimum points for Windows 10 to work, so don't expect your users to break any records using it with those specifications. Instead, we recommend that you have a dual-core processor rated to at least 2 GHz, anywhere from 4-to-8 GBs of RAM, and a 160 GB hard drive at the minimum.

Virtualize Your Data Via the Cloud

Of course, you also have the option to simply use virtualized solutions, rather than acquire new in-house hardware. Not only are virtualized servers more cost effective than purchasing a new in-house system, you have much more flexibility in the types of servers you can host. Microsoft Azure, for instance, offers virtual machine capabilities that cover the gamut of a business' needs.

It also should be said that virtualization also assists with budgeting for your IT, as the purchases you would have made otherwise are turned into predictable operating expenses, rather than a pricey capital expense; plus, with services like Azure, your solutions are maintained as a part of the cost, so when compared apples-to-apples, virtualization could easily be the less-expensive option for you to go with.

Empower Your Team with Microsoft 365

Admittedly, while Microsoft 365 won't do much to resolve your difficulties with Server 2008 R2, you can implement it quickly, which helps when you're trying to beat an End-of-Life deadline. As it offers a comprehensive assortment of…

Read the Rest Online!
http://bit.ly/2LluPxu

![Global Tech Solutions logo]

What to Include in a BYOD Policy
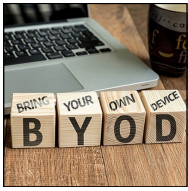
A Bring Your Own Device (BYOD) policy is something that many organizations have adopted, for a few good reasons: employee satisfaction, cost savings, and productivity boosts included. However, it's crucial that you don't just assume that you can adopt a policy like BYOD without establishing some ground rules that your employees need to abide by.

Here, we'll go over a few topics that your BYOD rules need to address.

Password Practices and Other Security

It's hardly a secret that some people utilize lax passwords - especially on their personal devices, where there isn't an IT department establishing policies to help ensure password strength. According to Pew Research Center, 28 percent of smartphone owners don't use a screen lock. Obviously, this isn't something that can be allowed in the business setting.

So, if your employees are going to use their personal devices to access business resources, you need to have a policy that their devices are set to lock after a certain period of inactivity, and require some form of authentication to unlock. Furthermore, the device should further lock down if an incorrect authentication code is input so many times.

Your policy should also include any required security solutions you plan to utilize as part of your mobile monitoring and management toolset. All devices should have antivirus installed, along with mobile device management and unified endpoint management solutions.

Provisioning and Network Security

Provisioning a personal device that is going to be used for company work helps to ensure a few things. Not only does it help to make sure that productivity applications are configured properly, it also helps to boost your security. Furthermore, your network needs to allow your employees' devices to access the business network - not just a guest network you have set up. Of course, there should be procedures and safeguards in place to ensure that this is done securely.

Tracking, Remote Access, and Data Wiping

Accidents happen, and devices can be lost - and sometimes, stolen. Furthermore, any device that is attached to a company network and has accessed illegal content could possibly leave the company liable - especially if this content was accessed via the company network. Your IT team should have the capability to monitor what websites and content each device included in a BYOD strategy has accessed, as well as to remotely access these devices to help ensure their security should they wind up missing. It also helps if they can implement updates to work solutions and security measures.

If worse comes to worse, it is beneficial to be able to delete all of a device's data remotely - that way, even if it is stolen, your data won't be at risk for as long. This also comes in handy if an employee is ever to leave your employ and you want to make sure they no longer have your data (or access to it).

BYOD can offer significant benefits to any organization. To learn more about putting a policy in place at your business, give Global Tech Solutions a call at (800) 484-0195.

Read the Rest Online!
http://bit.ly/2DRV2zF

We partner with many types of businesses nationwide, 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.

Abraham Brown
CEO

Tech Trivia
Google + was developed under the code name "Emerald Sea".

Global Tech Solutions

2964 Nostrand Avenue
Brooklyn, New York 11229

Voice: (718) 360-2000

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

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

WHO HELPS YODA OPEN PDF FILES?
ADOBE-WAN KENOBI!