AUREUSCONNECTIONS
THE TECHNOLOGY NEWS SOURCE FOR YOUR BUSINESS

QUARTERLY Newsletter

Fall 2016 | Vol. 2, Issue 4 | www.AureusConsultants.com | Phone: (209) 230-5818

Inside This Issue...

5 EASY THINGS YOU SHOULD DO TO PROTECT YOUR BUSINESS TODAY

Let's face it - no one likes to think about bad things happening to them, much less plan for them. But if you wait until after disaster strikes, you could be caught off guard. Here are some simple things you can and should be doing to protect your business:

Review Your Business Insurance *Carefully.*

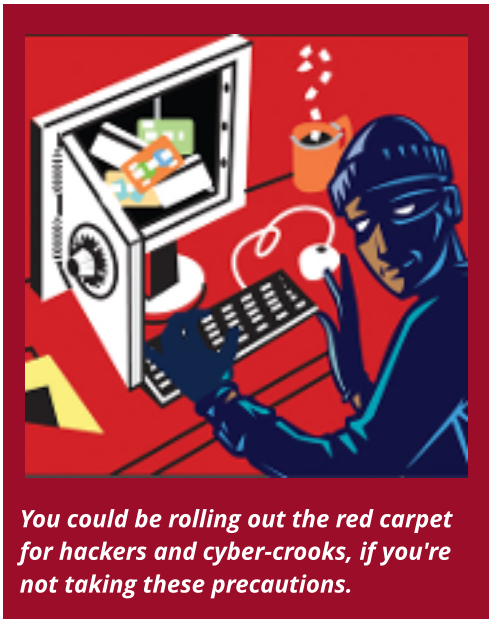
Most businesses carry some type of general liability insurance that would pay them if their building and the things in it were damaged. However, many businesses do not have enough coverage to replace all the computer equipment and devices, desks, art, supplies and other things they've accumulated over the years that are housed in their office. Make sure you review your policy every year and keep in mind new additions and assets you've accumulated during that year.

Consider Cloud Computing.

One of the biggest advantages of cloud computing is that your data and assets are stored off-site in a highly secure, high-availability data center, with failover and redundancy built in. That means that if your building were destroyed and you had to evacuate, or if your server melted down due to an unexpected hardware failure, everything you've worked so hard to create over the years is safe and not a sitting duck in your unsecured closet or server room.

Secure Your Data.

Making sure your data is protected from theft is a never-ending battle you don't want to lose. Companies that get hacked and expose sensitive client and employee data can face severe penalties, lawsuits and massive loss of credibility in the marketplace. Make sure you never have to send an e-mail to your customers explaining the bad news that a hacker accessed their info through you. Further, if you keep any sensitive information (even passwords to portals containing sensitive information) on portable laptops, phones and other devices, make sure you have a way of controlling and safeguarding that information.



You could be rolling out the red carpet for hackers and cyber-crooks, if you're not taking these precautions.

Write A Simple Disaster Recovery Plan.

The key word here is "simple." If your plan gets too complicated or difficult, you won't do it. But, at a minimum, think of the disaster that is most likely to happen and that would have a severe and negative impact on your company's survival.

Review Your Employees' Internet Policy.

With so many people "addicted" to Facebook and Twitter, it's important that your employees know where the line is in what they can and can't post online. We also recommend content-filtering software to block content and websites you don't want employees visiting during work hours.

End-Of-Life Applications Are Risky For Your Business!

Most IT experts will tell you how important it is to patch your systems in a timely manner but, when an application is no longer supported by its manufacturer, it can become a serious security risk to your enterprise.

Often Overlooked

Even though the vast majority of malware exploits the known vulnerabilities of out-of-date software, businesses often allow these end-of-life applications to continue to run on their systems. Many times this is simply because no one is using these apps and they've overlooked removing them.

Malware is Evolving

Just like real viruses, CryptoWall and other types of malicious software are always evolving and becoming more sophisticated. Malware has become a penetration tool for hackers and cyber crooks who are looking for ways to exploit your network.

Attackers Will Exploit

Attackers know that regular malware can be detected by any good anti-virus program, so they tend to use it initially for launching an intrusion. Once the infection is on your system, the attackers can exploit your end-of-life applications because they have not received the latest updates for protection against newer viruses.

Risking Your Business

If you still have unused end-of-life applications on your system, you could be risking your business!

CORTANA GETS A WHOLE LOT SMARTER
WINDOWS 10 ANNIVERSARY UPDATE NEWS

Can you believe Windows 10 is already celebrating its first birthday? Released in August, here are some highlights of what you'll find in the Anniversary Update:

CORTANA GETS AN UPGRADE

In an effort to compete with *Siri*, *Google Now*, *Alexa*, and others, Microsoft has continued to expand what *Cortana* is capable of. With the new update, *Cortana* can be started from the lock screen and is able to push notifications and text messages from your mobile device to your desktop. You can also install *Cortana* on your android, so it doesn't require a Windows phone. When you are signed in with the same Microsoft account across your devices, *Cortana* can act like a personal assistant and catch schedule conflicts or even order your dinner.

WINDOWS HELLO GETS IMPROVED

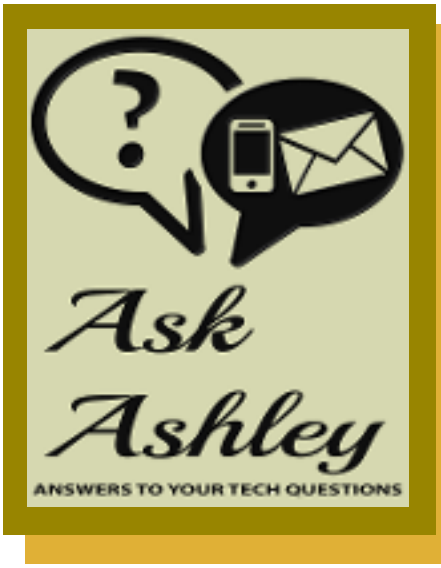
While Windows already supported logging into your laptop with fingerprint sensors, the new update now extends fingerprint security for Windows apps and websites on Microsoft Edge - provided you have the necessary hardware. *Windows Hello* will also now let you unlock your PC with companion devices, such as your phone, a USB device, or even a *Microsoft Fitness Band*.

WI-FI SENSE FEATURE GETS TRASHED

Microsoft has removed the controversial password sharing feature of *Wi-Fi Sense*, citing that it wasn't worth the effort to keep it around since very few people actually used it. *Wi-Fi Sense* isn't completely gone but now it will only connect to public hotspots and it won't offer to share your Wi-Fi credentials with others.

WINDOWS DEFENDER ADDS SECURITY

Before this update, *Windows Defender* would automatically disable itself if you installed another anti-malware program. Now, *Windows Defender* has a new "Limited Periodic Scanning" feature which can scan your system occasionally, even if you have another anti-virus program installed. Just head to *Settings > Update & Security > Windows Defender* and turn on the "Limited Periodic Scanning" feature to enable this. This option will only appear if you have another anti-virus program installed, and it isn't on by default. If you're only using *Windows Defender* as your anti-virus, it's already scanning your computer–both with scheduled and real-time scans.



QUESTION:

If my organization is still running Windows 7, *do I need to upgrade to Windows 10 at this time?*

Do you have a question for Ashley? *Email: asmithj@aureusconsultants.com*

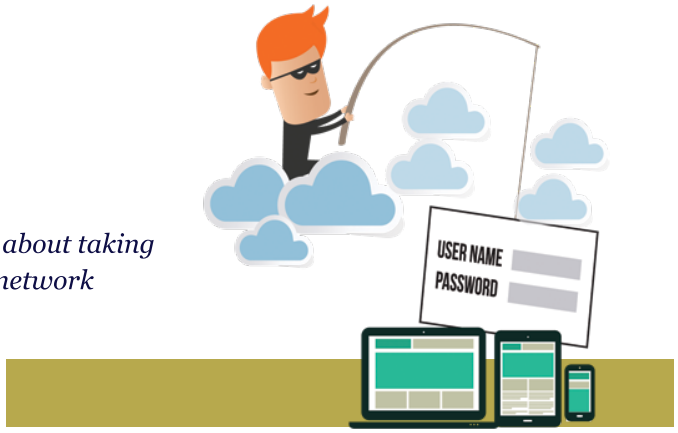
ANSWER:

It depends. If you have software or line of business applications that only run on Windows 7, then do not upgrade (Windows 7 will be supported up to January 14, 2020). If not, then upgrade to Windows 10 one computer at a time for an easier migration and future-proof installation. If you have a server, make sure it is running Microsoft Server 2008 R2 (or SBS 2011) or later that supports Windows 10. Also, make sure you are running the Professional version of Windows 10 which is designed for business use and seamless server integration.

FOUR STEPS YOU CAN TAKE TO AVOID IDENTITY THEFT IN YOUR BUSINESS

COULD YOU FINANCIALLY SURVIVE IF YOUR BUSINESS AND PERSONAL IDENTITY WERE STOLEN?

Many small business owners tend to ignore or simply don't know about taking steps to secure their personal and company information on their network from online hijacks. By then it's too late and the damage is done.



STEP 1: MAKE SURE YOUR BACKUPS ARE ENCRYPTED

It just amazes me how many businesses don't have the security of encrypted backups. Encryption takes every little keystroke that you type and every little piece of data in your computer and turns it into dozens – or hundreds – of other characters. For example, just one letter "A" could turn into 256 different letters, numbers and symbols when it is encrypted. It basically makes it a whole lot more difficult for a hacker to figure out what the data is. On the other hand, if you DON'T have encryption, you are opening yourself up to a BIG risk of your identity and other important data being swiped. That is why it is so important to make sure your backup is properly secured.

STEP 2: MAKE SURE YOUR VIRUS PROTECTION IS ALWAYS ON AND UP-TO-DATE

With virus attacks coming from spam, downloaded data and music files, instant messages, web sites and e-mails from friends and clients, you cannot afford to be without up-to-date virus protection.Not only can a virus corrupt your files and bring down your network, but it can also hurt your reputation. If you or one of your employees unknowingly spreads a virus to a customer, or if the virus hijacks your e-mail address book, you're going to make a lot of people very angry.

STEP 3: SET UP A FIREWALL AND UPDATE IT REGULARLY

Small business owners tend to think that because they are "just a small business," no one would waste time trying to hack into their network, when nothing could be further from the truth.

These individuals strike randomly by searching the Internet for open, unprotected ports. As soon as they find one, they will delete files or download huge files that cannot be deleted, shutting down your hard drive. If the malicious programs can't be deleted, you'll have to reformat the entire hard drive, causing you to lose every piece of information you've ever owned, UNLESS you were backing up your files properly.

STEP 4: UPDATE YOUR SYSTEM WITH CRITICAL SECURITY PATCHES AS THEY BECOME AVAILABLE

If you do not have the most up-to-date security patches and virus definitions installed on your network, hackers can access your computer through a simple banner ad or through an e-mail attachment. Not too long ago Microsoft released a security bulletin about three newly discovered vulnerabilities that could allow an attacker to gain control of your computer by tricking users into downloading and opening a maliciously crafted picture. At the same time, Microsoft released a Windows update to correct the vulnerabilities; but if you didn't have a process to ensure you were applying critical updates as soon as they became available, you were completely vulnerable to this attack. It is an EASY way for someone to gain access to your information and steal your identity.

The Gold Standard Spotlight

Murphy & Brawley, LLP is a law firm specializing in the areas of business law and estate planning. Mike Murphy and Mason Brawley both grew up in Merced. After starting their careers in the Bay Area, they both returned home to practice locally and opened their office in Downtown Merced in 2014.

Murphy & Brawley hired Aureus Consultants to establish their office network and back-up systems and regularly consults with Aureus to troubleshoot issues and upgrade their technology.

Mike and Mason both offer free consultations to new clients. We encourage you to contact Murphy & Brawley, LLP for your business and estate planning legal needs.

MURPHY & BRAWLEY
ATTORNEYS AT LAW

2039 CANAL STREET
MERCED, CA 95340
(209) 349-8030
WWW.MURPHYBRAWLEY.COM

FREE NETWORK SECURITY CHECK

- Pinpoint any exposure or risk in security against potential threats
- Review your current backup systems to make sure they're working right
- Recommend ways to secure any vulnerabilities in your network
- Outline a comprehensive line of defense against ransomware attacks

Visit: ***aureusconsultants.com/securitycheck*** and schedule your FREE Network Security Check today!

TREND MICRO™

Worry-Free
Business Security Services

Advanced malware and ransomware protection from Trend detects and blocks ransomware encryption activities!

DON'T WAIT TO BE A VICTIM, CALL NOW FOR A FREE QUOTE: ***(209) 230-5818***

NEED FASTER INTERNET???

COMCAST BUSINESS

B4B

BUILT FOR BUSINESS™

If you have ever watched the clock while you were waiting for your browser to load, or been frustrated with buffering and slow internet speeds in your business, then now is the time to end your worries!

As a Comcast Business Authorized Connector:

- **We work hand-in-hand with Comcast to give you the best deal with the most discounts.**
- **We can offer you the fastest Internet connection in the Merced area.**
- **We'll handle everything so you'll never have to waste your time calling an 800 number again!**
- ***PLUS, OUR LABOR IS INCLUDED WHEN YOU MAKE THE SWITCH!***

If slow Internet connections are slowing down your business, call (209) 230-5818 or visit www.*AureusConsultants*.com to schedule your FREE consultation today!

Editor in Chief

Ashley Smith-Jenkins, President / IT Engineer
asmithj@aureusconsultants.com

Ashley has vast experience in the information technology field relating to computer and network services, including web development. For the past 21 years, Ashley has provided computer consulting and implementation for his customers. Ashley is a CompTIA A+ Certified technician and holds a Bachelor's degree in Business Administration from the California State University of Fresno.

Aureus Consultants, Inc. is a computer consulting firm and IT Service Provider headquartered in Merced, CA. We offer the gold standard in providing professional IT services with the most affordable options for local small businesses.

Contact:

AuREUS Consultants, Inc.
P.O. Box 3529
Merced, CA 95344-1529
Phone: (209) 230-5818
www.AureusConsultants.com

AuREUS CONSULTANTS
The gold standard in IT.