pulse Technology Solutions

TECHMinutes

June 2017

Your Business Technology Information Source!

This Issue:

The Cloud Revolution: We've Seen This Before

Threats to Your Data Come From All Sides

Next Job on the Automation Chopping Block: Pizza Delivery

4 Enterprise-Level Security Solutions in One Convenient Package

How Software License Mismanagement Can Hurt Your Bottom Line

3 Ways Managed IT Keeps Your Business in Business

Next Job on the Automation Chopping Block: Pizza Delivery

Did you know that over 2,000 Domino's Pizza franchises in Australia, New Zealand, France, Belgium, The Netherlands, Japan, and Germany feature delivery by robot? Starship Technologies, a self-driving robotics company, announced on March 29th that they would be partnering with Domino's to revolutionize the...

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

About Pulse

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

Visit us **online** at:

newsletter.pulse.tech

The Cloud Revolution: We've Seen This Before

As technologies emerge and trends change, organizations face massive paradigm shifts involving the tools and methods they use to conduct business. Right now, we're in the middle of one of the most significant shifts in decades; more and more businesses are relying on cloud computing.

The Basics

Cloud computing is a very broad term describing the usage of off-site computing. Essentially, when you use a cloud-based service, you are using someone else's computer to store and process data. Just for reference, let's say you are using Bob's computer.

Bob basically rents some of his computer's resources to you. Depending on the cloud provider, they might sell computing resources based on storage, processing power, bandwidth, or just how many accounts you need. In order for Bob to keep you as a customer, he needs to have these computing resources readily available. They need to be safe and secure. On top of that, Bob needs to sell you the computing resources for less than you'd pay for purchasing them yourself, taking into consideration the cost of managing, maintaining, and protecting your IT investment.

Those last few points are all the difference. Uptime and security are crucial for small business success, and businesses either need to proactively manage and maintain their IT or be

(Continued on page 3)

Threats to Your Data Come From All Sides

Just over a third (36 percent) of businesses don't back up business data at all, and apparently this number isn't keeping some IT providers up at night (not the case for us). Your businesses' data is precious, irreplaceable, and extremely expensive to lose. Let's talk about how delicate and dangerous it is to not have it backed up.

Hard Drives are Extremely Fragile

The device inside your computer or server that holds your data is easily the most sensitive and breakable component. Traditional mechanical hard drives work by spinning a spindle of platters at extremely high speeds. These platters have a thin magnetic coating that stores your data. A tiny arm rests over the platter with nothing but a cushion of air holding it in place. The spinning of the platter keeps the magnetic head on this arm from touching the platter. If the head were to touch the platter while it is spinning, it would decimate your data.

Modern drives have plenty of safeguards to prevent issues, but like any mechanical device, wear and tear will happen, and outside forces like bumps and shocks can shorten the reliability of a drive. If your data is confined to one drive, it just takes one bad day to lose it all, and recovering the data could be impossible.

Users Make Mistakes

Let's say your company uses a Word document as a template for your sales proposals. Your sales team knows to make a copy of it, drop it in the client's folder, and edit it from there.

(Continued on page 2)

"Successful companies in social media function more like entertainment companies, publishers, or party planners than as traditional advertisers." – Erik Qualman

4 Enterprise-Level Security Solutions in One Convenient Package

How big a role does security play in your business's network management? If it takes a secondary role more in favor of operations, you might want to reconsider why this is the case. After all, your organization's critical assets--namely sensitive data like employee information, payment credentials, and usernames or passwords--all hold immense risk for exploitation from hackers. Therefore, even if you don't fear a potential attack, you should at least consider it as a possibility.

To optimize security on your business's network, we often recommend what's called a Unified Threat Management (UTM) tool. This combines several of the most important enterprise-level security solutions into one package for maximum network protection. Here is what a UTM contains and why it's important for your organization.

Firewalls

Firewalls are beneficial in that they keep threats out of your network in the first place, meaning that they don't even have the opportunity to access your network and cause trouble for your business. Firewalls act as the virtual bouncers of your network, keeping dangerous traffic from entering while keeping threats in one place so that they can be thrown out or eliminated quickly.

> ***"...employee information, payment credentials... all hold immense risk for exploitation from hackers... if you don't fear a potential attack, you should at least consider it as a possibility."***

Antivirus

An antivirus solution complements a firewall by eliminating threats that do manage to slip through the firewall's grasp. An enterprise-level antivirus solution can identify and eliminate threats of all types; malware, viruses, trojans, and so much more. It's a great way of mitigating risk for your organization by ensuring that you take quick action against any potential threats. The big difference between a centrally located antivirus such as this, compared with standard consumer-grade antivirus is that the updates and scans aren't up to your end users, making the process seamless without interrupting productivity.

Spam Blocker

Spam isn't just an annoying and problematic thing to find in your inbox, it can also be exceptionally dangerous. Hackers will often use spam to spread their malware, and advanced phishing schemes are used to collect credentials and steal sensitive information from unwary users. Enterprise-level spam blockers are used to prevent spam from even hitting the inbox, allowing no room for error on your users' behalf. Of course, advanced threats often know how to dodge these blockers, so training for your employees is still ideal.

Content Filter

The Internet holds countless threats that can put your organization at risk, including malicious websites designed to harvest credentials, and downloadable attachments that can infect your network with ransomware before you know what hit it. The best way to keep users from accessing these dangerous sites, along with time-wasting websites that hold your business back from succeeding, is a content filter. You can block malicious online threats while keeping your employees from accessing social media (YouTube, Netflix, etc.) killing two birds with one stone.

Your organization can't take any risks with its network security. To learn more about a Unified Threat Management solution, give us a call 239-362-9902.

Share this Article!
http://bit.ly/2pFtd5X

Threats to Your Data Come From All Sides

(Continued from page 1)

That is, until someone makes the mistake of editing the original copy and saves over the file after making major edits to it. Now someone needs to scramble to restore the file by hand. If it were backed up, you could simply restore the file from your backup.

Ransomware is Evil

Everyone knows they need to protect their computer with antivirus, but there are threats out there that can penetrate commercial antivirus solutions. One of the most common is ransomware, like Cryptolocker and Cryptowall. Both work in a similar fashion, commandeering your PC and locking your files from you unless you fork over cash. They can even infect other computers on your network and external storage devices, which could include your backup depending on your setup. Storing an off-site backup is critical for preventing this.

Is Anyone Checking Your Backup?

If your IT company set up a backup solution, is it being tested and maintained? If you don't have an agreement or aren't getting a bill for it, the answer is probably not. Just like any computer, things can go wrong with your backup solution. Backups should be tested and evaluated regularly, or else you might find yourself out of luck in the event of an emergency.

Our powerful backup and disaster recovery solution can be just what you are looking for to protect your business from the myriad of threats out there. Call Pulse Technology Solutions's certified technicians today at 239-362-9902 to learn more.

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

The Cloud Revolution: We've Seen This Before

(Continued from page 1)

prepared for unexpected costs when problems occur.

Bob can do something that most small businesses can't. He doesn't just manage the computer he's renting to you. He's managing hundreds or thousands of virtual computers, located all in one data center. This brings the costs-per-unit down. While keeping everything secure is still not necessarily an easy task, Bob is able to control the infrastructure as a whole and invest in higher-end solutions that a small business might not be able to justify for a smaller IT footprint.

This tends to mean better security, better capabilities, and even cutting-edge solutions that keep your business in line with your competitors for less money.

So why does this sound so good?

This is Nothing New

If we look back at the late 1890s, long before businesses were worried about computers crashing or malware infections, they were concerned with generating their own electricity. Factories required onsite generators that were expensive, inefficient, and difficult to maintain. In some cases, staff needed to be kept on hand just to keep operations moving. If a generator failed, productivity would stop.

At the turn of the century, in Chicago, the Edison Power Company changed all that. They were able to provide reliable, cleaner electricity to factories for less money in the long run. The cost per unit was cheaper for the Edison Power Company because they could manage and maintain their infrastructure and focus on the specialized staff and equipment to do so. In just 20 years, utilizing the power grid was commonplace and the paradigm shift made its full course.

The Cloud is Essentially the Same Thing

Where businesses today wouldn't imagine producing their own electricity in-house, years from now many businesses will likely have the same thoughts about their IT infrastructure. With a rapid shift from on-premise servers and infrastructure to cloud-based IT, and the explosion of mobile computing, many businesses are moving away from servers and even traditional desktops altogether. Services like email, document management, line-of-business applications, and much more are all being delivered through the cloud, with more features and security at lower costs.

This future isn't far off - many businesses have been virtualizing their servers and desktops for years, and replacing expensive in-house systems with cloud-based solutions where the responsibilities of managing and protecting the infrastructure are no longer on their shoulders.

It's time to take a serious look at your infrastructure. Your next major…

Read the Rest Online!
http://bit.ly/2pFeR5B

How Software License Mismanagement Can Hurt Your Bottom Line

Whenever you install software on your computer, you agree to certain terms put in place by the developer or vendor. Even free software, such as Google Chrome and Firefox, have terms that the end-user opts into during installation.

One of the most important terms business owners need to be aware of are those that pertain to software licenses; if you aren't, someone else will be.

How Software Licensing Works

Software licensing is everything but simple. Developers determine where and how often you can install the software, whether or not you can modify or redistribute it, and other terms. Installing the software means you agree to these terms. Most commonly, these terms are designed to protect the developer from having their software shared and distributed without them charging for it. This makes sense, it's theft.

Interestingly enough, there have been some pretty wacky terms snuck into the license agreements of some programs. One of our favorites is Apple expressly forbidding users from using iTunes to create missiles and nuclear weapons. While we hope our clients are not weaponizing iTunes, there is a much more realistic concern that business owners absolutely need to be aware of.

Negligence Can Lead to Huge Fines

Depending on the software, when you install it and "activate" it, the software might phone home to the developer to authenticate the license. If the software sees that it's been recently installed or is currently active elsewhere, it might report back and not let you use it. Alternatively, it might not immediately reveal that it sees multiple copies in use. The developer might even give you some lenience (sometimes you can install a copy on your work PC and on a laptop). If you don't understand the licensing, you won't know until the cease and desist letters come in.

Typically, software developers are prepared to catch this and offer ways for you to purchase additional licenses (although not all the time). They might even offer volume or site licensing which will help you save money when purchasing software for all of your employees. While you need to be careful not to upset the vendor by mistreating your software licenses, there are even bigger threats to watch out for...

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

3 Ways Managed IT Keeps Your Business in Business

In the natural course of doing business, an owner/operator will have to face many difficult situations, but none of these situations are as difficult as asking them to determine whether or not to close the doors of the business for good. Many problems could cause a business to fail, but it has to hurt the failing owner a little more when the solution for the problem was not only within his/her reach, it was affordable.

When we talk to our clients, they are normally well adept at managing (and mitigating) risk. They've taken quite a bit of it on by opening a business, and many of them understand that negligence in any aspect of their company can mean curtains for the business. We like to think that's why they choose us, we work hard to improve their operational capabilities with properly-functioning technology; and, we have the solutions they need to ensure that if something unfortunate were to happen with technology, that they are protected.

Managed IT services; or, the outsourcing of IT support and services is not a new concept, but it is one that not enough small business owners consider. You've all seen the statistics, cybercrime is way up and businesses of all types are firmly in the danger zone as they often hold assets that cybercriminals are looking to acquire: financial information and Personally Identifiable Information (PII). This is exactly why small businesses deal with over 4,000 cyberattacks a day; and, why you absolutely need to have a cyber security plan for your business, as well as a continuity plan if things end up going south. Here is what Pulse Technology Solutions supplies to ward against this type of tragedy:

Proactive Monitoring and Maintenance

No need to fix a problem that isn't a problem in the first place. Small businesses today deal with all types of malware, social engineering, and other attacks that aim to steal your client's data, breach your network, and decimate your relationship with your customers. With our remote monitoring and management tool, we are able to proactively monitor and maintain your business' network and every piece of hardware attached to it. This way simple (and unavoidable) issues like a failing hard drive won't become problems. Maintaining functioning technology can go a long way toward bridging the gap between breaking even and being profitable.

Comprehensive Threat Management

Every small business needs to understand what they are up against. It's not pretty. With thousands of cyberattacks a day, some so powerful that they could potentially take down the entire Internet, businesses have to have (at the very least) a cursory threat management platform in place. A strong multi-layered approach, equipped with an enterprise-level firewall, spam protection, content filtering, and VPN access can go a long way toward keeping intruders out of your network.

Backup and Disaster Recovery

If you don't understand the value of a backup system for your company's data, let us spell it out for you as simply as possible. If you lose your data in some sort of cyberattack (or for any other reason), and you don't have a reliable backup solution in place, you can flip a coin to see if your business will survive. It is that dire. To protect your business from...

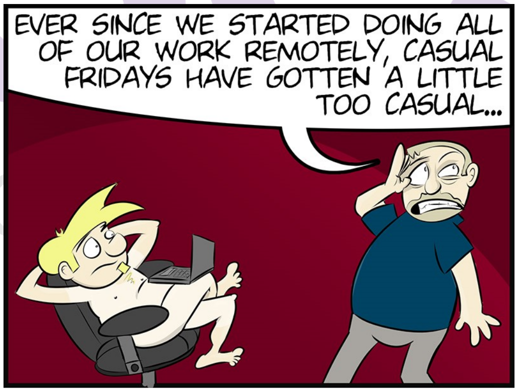
Read the Rest Online!
http://bit.ly/2pdoQgq

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.

James Ritter
Founder & CEO

PULSE TECHNOLOGY SOLUTIONS
ANNIVERSARY
10
YEARS
REPUTATION OF INTEGRITY & TOP QUALITY SERVICE

Tech Trivia
One in six consumers currently own and use wearable technology.


EVER SINCE WE STARTED DOING ALL OF OUR WORK REMOTELY, CASUAL FRIDAYS HAVE GOTTEN A LITTLE TOO CASUAL...

Pulse

12611 New Brittany Blvd.
Bldg# 18 Fort Myers,
Florida 33907
Voice: 239-362-9902

Visit us **online** at:
newsletter.pulse.tech

newsletter@pulse.tech
facebook.pulse.tech
linkedin.pulse.tech
twitter.pulse.tech
blog.pulse.tech