Paradigm Computer Consulting

TechAdvisor Newsletter

March 2016

Your Small Business Technology Information Source!

This Issue:

Why BYOD is an Important Industry-Changing Trend

Mobile devices are challenging the traditional perception of the office environment. When employees bring their own devices to work, this is called Bring Your Own Device (BYOD), and it's an increasingly popular trend...

Read the Rest Online! http://bit.ly/20GbWsE

About Paradigm

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:
paradigmcomputer.com

3 Ways Remote Technology Benefits Both Your Employees and Your Business

In an age when working remotely is a commonly accepted practice, many organizations are still skeptical about letting their employees work from home. They think that doing so will disengage them from the workplace environment and that they'll be too distracted to perform their work to specification. Yet, businesses that aren't flexible on this issue could be missing out on several significant cost savings.

Your Energy Costs Decrease

When you have an office full of workers, there are a lot of expenses that are used to help them perform their duties. Depending on the environment, you have to either heat the office in the winter, or air condition the office in the summer. All of your organization's workstations consume a significant amount of electricity, which can eat up a lot of your assets. That's not to mention lighting, the purchase of snacks, coffee, and other boons that employees might benefit from while at the office.

If you allow your employees to work from home, that's energy that's not used. Energy that's not used leads to more savings on your part, and your organization's bottom line will increase as a result. You'll see yourself spending less money on energy and earning more cash.

(Continued on page 3)

The Cloud Makes Everything Easier, But Only If it's Managed Properly

As an increasingly more important component of the modern technology infrastructure, the cloud can be a daunting new addition to any organization's business strategy. Yet, many businesses still haven't made the jump to the cloud, perhaps out of fear that their use of the cloud won't significantly benefit them.

Basically, you can have an idea of how successful a cloud computing endeavor will be for your business, but you won't know for sure until you take a risk and try it out for yourself. Many of the world's top services, like Amazon and Netflix, have achieved mammoth success thanks to the advent of cloud computing. Your business can achieve a similar level of success in your chosen industry, but only if you're willing to take new and daring risks with how you use your cloud solution.

That being said, you should still approach the cloud level-headedly by doing your research and understanding what exactly you want to achieve with your cloud solution. We recommend that you thoroughly consider each of these three unique cloud computing options.

The Public Cloud

Many SMBs are turning to the public cloud for their cloud computing needs. This is usually because the public cloud has the functionality that they need, without requiring the in-

(Continued on page 2)

The Cloud Makes Everything Easier, But Only If it's Managed Properly

(Continued from page 1)
depth maintenance and management that an in-house computing system would require. This is the primary benefit of the public cloud; you get all of the base functionality of a cloud solution, without all of the hassle of managing it. Where it falls short, though, is the lack of additional security features that the private cloud offers.

Simply put, public cloud solutions are reliable, but by definition, pretty cookie-cutter. They are designed to support lots of customers and get a particular type of job done. The customers don't have control over where specifically their data is hosted, what hardware it runs on, or how it's protected.

The Private Cloud

Business owners who turn to the private cloud tend to be more controlling and security-minded than those who are fine with the public cloud. A private cloud tends to be hosted in-house on company hardware or managed externally at a secure data center. Private clouds offer more control over the configurations and setup of your cloud infrastructure, making it ideal for those who want to know exactly what's going on with their cloud solution, and why. Plus, private clouds can be combined with additional security measures, like a Unified Threat Management (UTM) solution to optimize data protection, where the public cloud controls all of these things for you.

The Hybrid Cloud

Businesses that want the best of both the private cloud and public cloud have the option to use a hybrid cloud solution. These are designed with the ease-of-use of the public cloud in mind, but also allow for enhanced security management similar to the private cloud. It's ideal for organizations that need a little bit of both, without compromising on functionality.

If you're unsure about how your business should take advantage of the cloud, Paradigm is happy to assist you. We can identify major pain points that can be addressed by cloud computing, and assist with the planning and implementation of your chosen hosted solution.

To learn more, give us a call at (603) 647-8614.

Share this Article!
http://bit.ly/20RMuwZ

Your Network Needs a Virtual Bouncer to Keep Threats Out

Firewalls are one of the most common IT security measures on the market today, and for good reason. They act as the first line of defense against any incoming threats, and without them, your organization would have to deal with one data breach after another. Of course, that's only if you're taking advantage of a proper firewall; if not, you should seriously consider doing so as soon as possible.

In general, cyber security is an important asset to invest in, especially with the number of data breaches growing by the day. 2015 saw so many high-profile hacks that it feels like nobody is safe. When major institutions like government offices and healthcare providers have trouble keeping hackers at bay, the unanimous assumption is that hacks can, and will, happen, regardless of what industry you're in and how well you're protected. It's becoming painfully obvious that businesses that fail to utilize any security solutions are at tremendous risk of data compromisation.

Well, it turns out that any business can optimize its cybersecurity measures, and it begins by integrating a simple firewall. Here's how a firewall can benefit your organization.

The Benefits

Firewalls are absolutely critical for any business that wants to maximize its cyber security. Firewalls have the ability to detect unwanted network activity, refuse access to your network, and send notifications to a system administrator. Firewalls essentially monitor data that flows both into and out of your network, scanning for threats and preventing them from entering your network. If any threats are detected on the inside, the firewall can prevent them from exiting the network, allowing for efficient elimination. The idea is that the firewall should be able to identify potential threats and inform the proper administrators before excessive amounts of damage accrue.

There's no reason for a business to not be using a firewall. As the most basic of cyber security measures, it's easily configurable to suit the needs of your business.

What They Don't Protect You From

Firewalls aren't perfect. While they're great for keeping threats out of your network in the first place, they aren't going to do much to eliminate threats that have already made their way into your infrastructure. This is why firewalls are often paired with other security solutions like antivirus software, that allow for the detection and elimination of potential threats within a network…

Read the Rest Online!
http://bit.ly/20RMFbA

3 Ways Remote Technology Benefits Both Your Employees and Your Business

(Continued from page 1)

Your Operational Costs Decrease

When you hire new employees, unless you have workstations, laptops, and other devices on hand for them to use for their jobs, you'll have to purchase new hardware for them. You don't need us to tell you that new hardware is expensive, same goes for software solutions. Outfitting your employees with the tools they need, while your responsibility, can drain your budget.

If your employees are using their own technology to handle their day-to-day tasks, you won't run into this problem. They'll be taking advantage of their own technology, which adds a whole new level of depth to your organization's budget. Granted, you'll want to be using a mobile device management solution and a BYOD policy to ensure that these devices aren't compromising your network security, but equipping your employees with these solutions is simple enough to warrant consideration; especially if you have an outsourced IT department that's willing to help your organization get this technology set up.

Your Employees Will Be Happier

Employees that are capable of doing their jobs from the comfort of their own homes might like working for you, but the effort and time it takes to get ready for work and drive to the office can take its toll over time. Plus, if their job is especially repetitive and doesn't require much oversight, they can quickly become discouraged about their situation. It's a known fact that happier employees are more likely to stick around for long periods of time.

Letting your team members work from home has been known to improve both morale and work ethic. At home, there are less distractions for employees, especially if your office is open and there are several people who work in the same room. Your employees will appreciate the peace and quiet of their own home, and will be able to concentrate better on the task at hand. Furthermore, your employees will be more likely to do something that they've been trying to do for years; save some money. Since they don't have to spend it on gas to get to the office, they'll have some extra cash in their wallet, which is enough to make anyone smile.

If you decide to let your employees work from home (and you should), you'll want to make sure that they're equipped with all of the technology and access to critical information and data that they need in order to perform their daily duties. There are several technologies that aid in this endeavor, like a virtual private network (VPN), Voice over Internet Protocol (VoIP), cloud-based data storage, and virtualization services. Most important of all is the mobile device management solution, which helps to keep employee devices and applications from accessing information that's sensitive to their user role.

If you want to equip your business's employees with the technology required to work remotely, give Paradigm a call at (603) 647-8614.

Share this Article!
http://bit.ly/20RLLvx

How to Leverage the Benefits of Mobile Devices While Negating the Associated Risks

Mobile devices have taken the workplace environment by storm, and you'd be hard-pressed to find anyone who doesn't use their smartphone, laptop, or other device for work purposes. This trend, called Bring Your Own Device (BYOD), helps employers spend less on new solutions, but it also presents a risk that needs to be managed: the Internet of Things (IoT).

According to a study by Tech Pro Research, 59 percent of businesses allow the use of personal devices in the workplace, while only a modest 28 percent were adamant enough to claim that they have no plans of allowing personal devices in the office. Only 13 percent plan on changing their policy over the next year.

We think it's safe to say that BYOD will continue to grow more popular as time goes on, but the businesses that are vehemently opposing BYOD have valid reasons to be concerned about employee devices. Furthermore, the use of Internet of Things devices, which are known for sharing data amongst each other, is increasing in popularity.

Even if a significant portion of business owners have no plans to integrate the IoT with their business, they might not have a choice if employees bring them into the office unknowingly. Therefore, it should be a top priority to protect your business's network from the potential harm these devices can cause. This is why it's important to manage the benefits of BYOD alongside the risks associated with the IoT.

Benefits of BYOD

The Bring Your Own Device revolution provides several great benefits for businesses that want to improve the quality of their operations.

- **Lowered equipment costs:** If you're allowing employees to bring in…

Read the Rest Online!
http://bit.ly/20RMNIa

Paradigm
Computer Consulting

Are Vigilante Hackers a Threat?

2015 was a brutal year for major corporations, as one by one they fell victim to hacking attacks. Major organizations like Blue Cross Blue Shield, Anthem, and even the United States Office of Personnel became victims of major hacking campaigns. A fact that's often lost amongst these details is that not all hackers use their skill for evil actions, even if they are still illegal.

As a matter of fact, there are many hacking organizations that use their skills for the benefit of mankind. Even though this type of "vigilante" activity is frowned upon, it doesn't help that pop culture icons like Batman, the Green Arrow, and pretty much any fictional superhero in existence defy these laws. There are times when it seems like it takes a criminal to beat a criminal, but we have to take into account what it means to let these vigilante hackers get away with these acts.

In many cases, the organizations and political entities that these "hacktivists" target are difficult for authorities to track down and punish. Hacktivists tend to take the fight to exceptionally dangerous organizations or individuals. The recent hacking attacks of ISIS at the hands of high-profile hacking group Anonymous come to mind, in which Anonymous targeted the terrorist group's social media sites, which are often used to gather and recruit followers. Just last October, Anonymous also revealed the identities of several suspected Ku Klux Klan members.

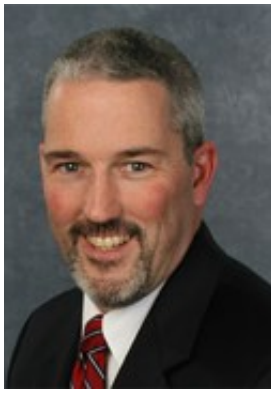
While it works in the movies, the presence of vigilante hackers reveals a major flaw in the way that society handles questionable online activity. We, as a people, have allowed the Internet to become a place that breeds danger, hatred, bigotry, and fear-mongering. Whether or not the activities of Anonymous are ethical is up for debate, though it needs to be mentioned that their activities are still illegal and shouldn't be condoned.

While your business is relatively safe from hacking attacks from hacktivists like Anonymous, there are plenty of bad hackers out there who want nothing more than to see your business fail. These bad hackers are after whatever private or sensitive data they can find, and you need to be prepared for them to take drastic measures to steal your data. The best way to protect your business's assets is to utilize a Unified Threat Management (UTM) solution. A UTM is a comprehensive solution that's optimized to protect your business from all kinds of threats. The UTM consists of enterprise-level solutions like firewalls and antivirus, plus other proactive measures like content filtering and spam blocking solutions. The UTM is designed to keep threats from accessing your network, and to keep your business out of the enemy's crosshairs.

While the UTM is great for maximizing network security, it should be mentioned that not every single threat can possibly be blocked. New threats are born every day, so you should treat every moment using online communication with a dose of skepticism. Your job as the…

Read the Rest Online!
http://bit.ly/20RNfGf

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.



Shawn Walsh
CEO

Tom E. Mitchell
COO

Paradigm Computer Consulting

40 South River Rd. #46
Bedford, NH 03110
603-647-8614

Visit us **online** at:
paradigmcomputer.com

newsletter@paradigmcomputer.com
facebook.paradigmcomputer.com
linkedin.paradigmcomputer.com
twitter.paradigmcomputer.com
blog.paradigmcomputer.com