Paradigm
Computer Consulting

TechAdvisor Newsletter

June 2016

Your Small Business Technology Information Source!

This Issue:

4 Security Best Practices that Every Employee Needs to Adopt

Security is a hot-button issue for all types of businesses, but cyber security is such a complex subject that it's difficult to jam-pack its many intricacies into one blog article. Sometimes understanding just a few **ways...**

Read the Rest Online!
http://bit.ly/220xZak

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

Avoid Getting Fined By Understanding How Regulatory

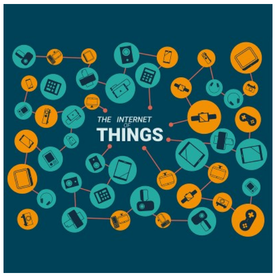
Technology is invading all practices, including those of medical offices and other health-related institutions like hospitals and dental offices. With the advent of electronic medical records (EMR) and their management systems, medical institutions are capable of eliminating the physical space required to store paper documents, and can instead easily store them in a digital environment. Unfortunately, this also brings its fair share of problems, such as regulatory compliance.

In other words, offices that don't take steps to adapt to these changing industry standards could be hit with compliance fines that break their budget. If your office doesn't take precautions to meet the various regulations put into place by HIPAA, HITECH, PCI, and other laws, and if the personal information for your office's patients is stolen by hackers, your business could be charged somewhere between $100 to $50,000 per record. You don't need us to tell you that this is an immense cost that's exceptionally crippling.

To help you keep your office in compliance, we've outlined some information about the various laws that you'll need to know about.

(Continued on page 3)

Making Sense of How the Internet of Things Applies to



The Internet of Things (IoT) is changing the way that businesses approach technology solutions, but its biggest impact might be in the consumer environment. With so many new devices connecting to the Internet and communicating with each other, it can be difficult to slap a label on the Internet of Things and associate it with the countless devices being created every day.

You can think of the Internet of Things as a group of mostly consumer-related devices that wouldn't ordinarily have Internet access, which have been granted connectivity and the ability to communicate with one-another. Gartner predicts that there will be approximately 26 billion IoT devices by 2020, with other aggregates putting the figure as high as 30 billion. In many cases, these devices are small and relatively inconsequential, like fitness-related wearable devices designed to monitor someone's heart rate or physical progress.

Other, more complicated Internet of Things devices could range from small household appliances, to computerized motor vehicles. Items like thermostats and refrigerators are commonly seen connecting to the Internet so that they can be controlled or monitored through a connected smartphone app, regardless of where the user is. Even in various industries, the Internet of Things is a tool that helps keep operations moving forward without a hitch. Take, for instance, these examples of how the IoT has been applied to specific industries:

- **Manufacturing:** Manufacturing plants use IoT devices to not only monitor progress of

(Continued on page 2)

What the country needs are a few labor-making inventions.
- Arnold Glasow

Making Sense of How the Internet of Things Applies to Different Industries

(Continued from page 1)

product assembly, but also for automating process controls, safety features, and security measures. In other words, the IoT devices used by manufacturers are mainly used to optimize the functionality of the plant.

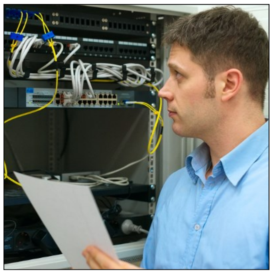
- **Energy management**: Some manufacturers are using IoT devices to monitor energy-consuming devices, and control these devices to ensure the maximum amount of energy is saved. Many of these devices are either set up to allow for remote control, or for access via a cloud-like interface.
- **Medical and healthcare**: On the medical front, IoT devices are capable of remotely monitoring medical equipment for information like blood pressure, heart rate, and other vitals. There are even pacemakers, insulin pumps, and other medical devices that are capable of connecting to the Internet and can be controlled remotely.
- **Building and home automation:** Some of the great IoT devices in the home automation industry include the aforementioned thermostats, garage doors, security cameras, lighting systems, air conditioning, and any other minor appliances that can be controlled remotely via a smartphone.

Security Issues and Discrepancies

With so much connectivity, security is a major issue and something to be considered when using any IoT device. Indeed, IoT devices present a unique challenge in keeping your network as free of them as possible, or at least minimizing your data's risk of being accessed by one of them. Since these devices communicate with each other, if even one of them is compromised, you could be looking at a potential data breach. This is why it's so important to both enforce a Bring Your Own Device (BYOD) policy in the workplace, as well as to manage the permissions and restrictions of devices on your network...

Read the Rest Online!
http://bit.ly/220zk0V

The Best Way to Manage Your Technology is also the Easiest!



Technology's incredible growth has brought about a need for technicians who are skilled enough to handle everyday maintenance. As time passes, technology grows more complex, and as such it requires more comprehensive maintenance. Eventually, innovators in the IT industry discovered that their services could be improved by preventing technology problems from happening in the first place. Enter: managed IT services.

We'll discuss the differences between traditional break-fix IT, and the managed services model that has changed the industry significantly.

How Break-Fix IT Works

Some businesses are known to run their technology into the ground. This means that they're using their technology, with all of its imperfections and warning signs, hoping that nothing will go wrong or break down. Companies like this hope to save money by dodging maintenances unless it's absolutely necessary. Ultimately this approach winds up being more costly.

For an analogy, look at the automobile. We all know that it works best when you're taking proper care of it by providing regular oil changes, replacing tires when they're needed, and other preventative maintenance. Yet, some people just don't take good care of their vehicles, and when they break down, it costs them a significant amount of money.

How Managed Services Work

Unlike break-fix IT, which takes care of problems as they appear, managed services are designed to detect abnormalities and issues before they become full-fledged problems. Doing so allows businesses to save money and time by outsourcing the upkeep and maintenance of their technology to a third party. By avoiding expensive technology problems, organizations can save further. For example, performing server maintenance is much cheaper and more efficient than dealing with an untimely and costly hardware failure in that same server.

The Benefits

As a busy business owner, one of the most limited assets that you have is time. There's only so much time in the day to manage your technology, and it doesn't help that you're restricted by a budget. Replacing a major piece of hardware can be crippling, especially if it's unprepared for. This is the biggest benefit of taking advantage of managed IT services: preventative maintenance is much more cost-effective and efficient than hoping for the continued functionality of your technology.

Basically, the big difference between break-fix IT and proactive managed IT is the fact that you'll be dealing with fewer technical hiccups due to regular...

Read the Rest Online!
http://bit.ly/220y122

Avoid Getting Fined By Understanding How Regulatory Compliance Works

(Continued from page 1)

HIPAA

Known as the Health Insurance Portability and Accountability Act of 1996, HIPAA is a set of compliance regulations that are designed to enforce electronic medical record privacy for patients. HIPAA covers, more or less, all healthcare organizations, the medical staff, and employees of the healthcare industry. This includes health insurance providers. Basically, HIPAA is designed to provide those who submit electronic medical records with rights to know how their information is being used and stored within the electronic medical record environment, and to ensure that health records and personal information is stored in accordance to the various security aspects of HIPAA.

HITECH

The Health Information Technology for Economic and Clinical Health Act was first introduced in 2009, and was designed to encourage medical practices to adopt technical solutions to their operational advantage. Specifically, HITECH revamped part of how HIPAA views user privacy. HITECH requires that organizations covered by HIPAA report data breaches of 500+ users to the United States Department of Health and Human Services, the media, and to the users affected. Furthermore, it changes the way that organizations handle the disclosure of electronic medical records, as well as how this information is used throughout the caregiving process.

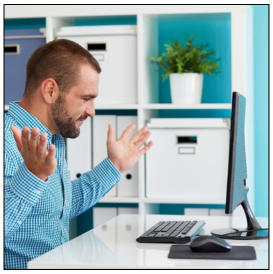
> ***"Basically, HIPAA is designed to provide those who submit electronic medical records with rights to know how their information is..."***

PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards that must be met before an organization can choose to implement major card-scanning technology systems. As credit card numbers are one of the hottest targets that hackers gun for, the main goal of PCI is to minimize and prevent credit card fraud. This applies to any organization, regardless of industry or product, that allows transactions to be completed with cards. Some examples of required protocol include maintaining a firewall that protects cardholder data, restricting access to card numbers on a "need-to-know" basis, and tracking and monitoring network resources, including what...

Read the Rest Online!
http://bit.ly/220y9yg

Let's All Move on From These 4 IT Frustrations



Technology is supposed to make things easier, yet it's a common source of frustration when it doesn't do what it's supposed to. As an IT company, we experience technology frustrations all the time, and we wish that many of these frustrations could just be eliminated altogether. In our opinion, here are four technology frustrations that need to go.

Passwords

If you follow the best practice of having a different password for every single account that is complex and hard to remember, then you're essentially left with a long list of complex passwords that is impossible to remember. Even if you utilize a password management tool like LastPass, you can still run into problems with passwords getting stolen, or having to navigate to a password page before you enter your account.

The crazy thing about passwords is that there are multi-factor and biometric technologies that can replace them (like retina and fingerprint scanning). These alternative technologies are easily accessible and can provide a more secure solution. Yet, here we are in 2016 and passwords are still the norm. You're asked to create a new one every time you sign up for anything online. We can do better. Let's move on from passwords.

Aggressive Promotion From Technology Vendors

Yeah, we're looking at you Java and Flash. Many "free" applications are free because they get paid by their sponsors to sneak in extra gimmicks like browser toolbars and new antivirus software into the installation. Yahoo and Ask toolbars are the most common. Most of the time you can opt out of these so-called bonuses, but if you aren't careful, you'll miss it and be greeted by a new application or browser plugin you weren't bargaining for.

This is reminiscent of Internet Explorer's much hated prompt, "Would you like to make Internet Explorer your default browser?" No IE, just let us open IE in peace so we can download Chrome already! Aggressive promotions like these are super frustrating...

Read the Rest Online!
http://bit.ly/220y0Lf

4 Ways to Avoid Distracted Driving While Still Being Productive With Your Phone

Business owners who spend a lot of time on the road, like during a commute or on a business trip, understand how difficult it is to use smartphones while driving. Despite the fact that it's illegal in many places, some people refuse to put down their phones and concentrate on the task at hand: driving. Doing so puts not only themselves, but everyone else on the road at risk of an accident, which can lead to expensive insurance payments and vehicle maintenance costs.

In general, it's safe to say that smartphones have been counterproductive to roadway safety. With drivers being constantly bugged by new notifications, be it through email or text message, one has to ask an important question: "Is it worth risking my life to respond to an urgent email while on the road?" The answer is clear; no, you absolutely shouldn't be doing so.

Not convinced? Consider these sobering statistics from the U.S. Department of Transportation:

- At any given daylight moment across America, approximately 660,000 drivers are using cell phones or manipulating electronic devices while driving, a number that has held steady since 2010.
- Ten percent of all drivers 15 to 19 years old involved in fatal crashes were reported as distracted at the time of the crashes. This age group has the largest proportion of driv-ers who were distracted at the time of the crashes.
- In 2014, 3,179 people were killed, and 431,000 were injured in motor vehicle crashes involving distracted drivers.

Alternative Solutions to Mobile Devices on the Road

To help you better take advantage of your smartphone, we've outlined a few potential solutions to this problem that continues to plague roadways. Keep in mind that we're not advocating for smartphone use while on the road; we just want to help people stay productive while also keeping themselves as safe as possible.

- **Bluetooth headsets:** If you absolutely need to talk on the phone while driving, you can make this easier by using a wireless headset that allows you to talk without holding the phone to your ear. Plus, if you're using a bluetooth headset, you can speak commands into the device to allow for hands-free navigation.
- **Voice recognition technology:** Some devices allow users to take advantage of hands-off technology like voice recognition. This allows them to focus on driving, while commanding the device to perform certain actions, like calling your office or sending a quick text message. You might still be somewhat distracted by your device, but at least your eyes will be on the road...

Read the Rest Online!
http://bit.ly/220yaSR

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

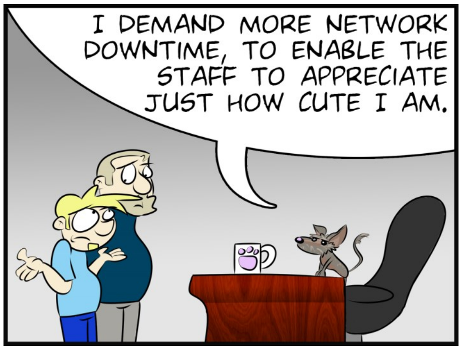
Tom E. Mitchell
COO

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


I DEMAND MORE NETWORK DOWNTIME, TO ENABLE THE STAFF TO APPRECIATE JUST HOW CUTE I AM.