This Issue:

Tech Term: Bandwidth Defined

The Internet has become an irreplaceable part of many business' operations, which brings the thought into question of how much you rely on it for your daily duties. Technology has changed the way that the Internet works for the better, but there is one part of its operations that still lies at the heart of it: bandwidth.

In the context of the Internet, bandwidth is used to measure the volume of information per unit of time that a transmission medium can handle. Basically, the more bandwidth your connection has, the faster data can be transferred. Bandwidth is typically measured…

Read the Rest Online!
https://dti.io/termbw

## Hackers Prey on Social Media Users

Social media has been an emerging technology in recent years, and has produced many threats. Hackers have learned that they can take advantage of these communication mediums to launch dangerous new attacks on unsuspecting users. With enough ingenuity on a hacker's part, they can potentially steal the identity of a social media user. Here are some of the best ways that your organization can combat identity theft through social media.

First, it helps to understand why social media is such an attractive vector of attack for identity thieves. For one, the anonymity provided by the Internet has long been a staple reason why it's been commonly used by hackers to steal sensitive information from organizations. This was (and still is) done through spam and scam emails, but nowadays, strategies have changed enough where individuals have to be more cognizant of their personally identifiable information, because by using social media constructs like Facebook, Instagram, Twitter, and the like, they are much more exposed. Enterprise-level spam filters are readily available to all kinds of organizations, prompting hackers to step up their game and create nefarious new ways of stealing information.

Spear phishing tactics were the result of these efforts. Intending to bypass the likes of spam blockers and content filters through seemingly legitimate sources, phishing tactics come in a variety of forms, with the most successful of these coming from sources that hide the true intentions of the one making the attack. The Internet can mask the true identity of hackers so that they can seem to be someone else, either in an email scam, social media attack, or otherwise. This is known as spoofing, and has been a infiltration tactic for decades.

Medical IT: How Is HITECH Doing?
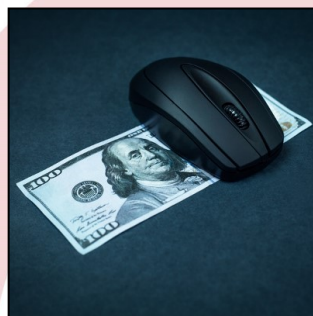
Compliance laws regarding the storage and dispersion of healthcare records were implemented with the intended purpose of urging healthcare providers to better take care of their patients' personal information, but how effective are they? Unfortunately, there are many providers that have failed to meet the standards for the HIPAA and HITECH compliance laws, and it has brought a hefty price tag along with it.

In 2016, the Office for Civil Rights (OCR) and the Department of Health investigated several data breaches that led to a considerable sum being claimed in response to violations of these compliance laws. In what totaled to 12 settlements following the investigations of data breaches caused by failure to comply with these laws, as well as one monetary civil penalty, these claims amounted to approximately $25,505,300 in fines.

Compare this to the more recent data. In 2017, there were only nine HIPAA settlements that produced a total of $19,393,000, as well as a single monetary civil penalty paid, a considerably smaller sum than the previous year. Clearly something is working here, but what is it? Perhaps it's the fear that being negligent with important data could mean a large sum raining down on the heads of those who fail to adhere to these laws.

25TH ANNIVERSARY
est. 1993

What You Need to Know About Data Recovery

Data backup is one of the most critical parts of protecting your business, but there are a lot of moving parts that need to be considered before implementing a solution. For example, did you know that data backup and disaster recovery are two different things completely? While they may both be involved in the business continuity process, the two represent equally important, yet disparate, parts.

Do you know what the major difference in them is? Data backup focuses on creating data backups in the event that you are to suffer from a loss incident. Disaster recovery is the act of actually restoring the data backup as well as any other operational function that may have been interrupted by a incident. In

many senses, data backup is the event that begins the process while disaster recovery ends it, ensuring that your organization recovers swiftly and efficiently.

There are several features that contribute to a successful data backup and disaster recovery solution. Here are just a few of them:

Recovery point objective: How much data needs to be backed up (and ultimately restored) in the event of a loss incident in order to continue or sustain operations? For a higher RPO, you will want to restore as much data as possible.

Recovery time objective: How long will it take to have your backed up data restored in order continue or sustain operations? Time is a luxury that you don't have when your organization's future hangs in the balance. The faster you can recover your data, the less downtime you'll suffer from.

Depending on the type of solution you

have in place, your RPO and your RTO will vary. A quicker RTO will likely result in a lower RPO, as the more data you need to have restored will cause longer recovery delays. You will have to alter your recovery plans based on your particular configuration. It is also worth mentioning that not all backup solutions are as effective as others.

Tape backup, the staple solution for many years, needs to be manually run in order for you to get back in business following a disaster scenario. Furthermore, due to the cumbersome nature of tape backup, it's possible to lose at least a day's worth of data. The alternative, network-attached data backup and disaster recovery (BDR) with cloud functionality offers faster recovery times and more thorough recovery options. All you have to do is restore the data to any device via an Internet connection…

Read the Rest Online!
https://dti.io/needtoknow

Hackers Prey on Social Media Users

In particular, social media can provide attackers with a lot of information without them working too hard. Think about the kind of information that you might have on your personal Facebook or Twitter feed. Do you have a phone number? What about an email address or physical address? Do you have any information about the musicians you listen to, or the books that you enjoy? All of this information (and more) can be used to help a potential scammer steal your identity and use it for various ill offenses - the gravest of which could be stealing your identity and using it to attack those you hold dear.

Imagine what could happen if someone were to steal the credentials to your social media pages and use them to impersonate you. They could fool all of your closest friends and family into giving up whatever information they are looking for. For example, they might be able to coax your parents or loved ones

into parting with personally identifiable information such as your Social Security number or credit card number, which could be used to open new lines of credit or make fraudulent purchases. Regardless, the threat posed by identity theft through social media is considerable, and you must take precautions to ensure that you don't fall for these traps in the future. Here are some ways that you can make sure this doesn't happen.

- **Be on the lookout for suspicious activity on your accounts:** If you suspect for even a second that your accounts have been compromised, be sure to change your passwords so that they can't be used to hurt those closest to you.
- **Look out for dangerous messages sent to you:** If you suddenly receive messages from those who you haven't heard from in a long time, and their behavior is suspicious, perhaps it's best to ignore these

messages or alert those who you think may be affected.
- **Limit the information you share on social media accounts:** Information can't be stolen if you don't choose to share it. Consider implementing more powerful privacy settings for your accounts.

Businesses are just as vulnerable to spear phishing attacks as individuals, if not more so. If you are like billions of others, social media has become an important part of your life, and quite possibly, your business. To ensure that you are doing what you can to protect yourself and your organization from the threats that social media and other innovative communications technologies enable, consider reaching out to the IT professionals at Directive.

Share this Article!
https://dti.io/preysm

Medical IT: How Is HITECH Doing?

(Continued from page 1)

What's even more interesting are the types of violations that led to these penalties. While the majority of these involve a failure to protect protected health information, or PHI, and its digital counterpart electronic protected health information (ePHI), there are a couple of outliers that are interesting to look at. Here are some of them:

- Insufficient ePHI access control
- Impermissible disclosure of ePHI
- Careless handling of PHI
- Multiple HIPAA violations
- Delayed breach notifications
- Lack of security management process
- Lack of a business associate agreement

The majority of the issues revolving around HIPAA and HITECH compliance come from an inability to secure mobile devices, failure to implement proper security processes, and delaying breach notifications for far too long.

As for HITECH specifically, a recent lawsuit was filed in federal court against 60 hospitals over alleged failure to adhere to the HITECH Act. Specifically, these hospitals failed to adequately provide records and documentation for 50% of their patients within three business days of the request. This is one of the specific requirements for securing funding through the HITECH Act, so you can understand that this was quite a big red flag for government.

Consequently, these 60 hospitals from the state of Indiana now face charges totaling over $1 billion for failure to provide records as required, despite receiving the incentive payments totaling around $324 million. Additionally, these hospitals face claims that they violated the Anti-Kickback Statute and the False Claims Act for claiming that they were HITECH-compliant, when in reality they failed to meet the requirements of the regulation. Not all practices fail to adhere to HIPAA and HITECH, though. Is your practice one of them? Answer with confidence today by reaching out to Directive at 607.433.2200.

Share this Article!
https://dti.io/hitech

Varieties of Smart Tech to Consider

How often do you see smart technology in headlines? The term is thrown around a lot, and it's because there are countless products circulating in both the consumer and business environments. These connected devices range from smart forks to smart cars, so you can imagine that there are a fair number of useful (as well as useless) applications of this technology. How has it changed in recent months, and what will smart technology look like in the future?

For Your Person

Smart products are produced for a variety of reasons with one of the more practical ones being monitoring your physical wellbeing. One of the best and most recognizable devices for this purpose is Fitbit, which has ushered other companies dedicated to health monitoring devices through the door. Health bracelets, watches, and smart fabrics all contribute to this trend of connected devices encouraging people to care

more about their health using technology.

These devices contain microprocessors, sensors, and energy sources, and they contain the hopes and dreams of engineers who have worked tirelessly to create some of the most compact technology solutions on the market today. These devices are so useful that there were 125 million wearables shipped in 2017 alone. Here are some of the most popular smart technologies on the market today:

- Fitness trackers: The most simple fitness trackers can count your steps and estimate calorie loss, as well as distance traveled, sleep quality, and speed.
- Smart watches: Some smart watches can track fitness information, as well as other features that work with other apps on your mobile device.
- Smart clothes: As you might imagine, most smart clothes are typically designed for use with fitness. There are self-cooling shirts that react to your body temperature, as well as yoga outfits designed to help your yoga posture.

For Transportation

Automobiles have also made great strides in smart technology. You'll see cars that offer everything from heads-up displays to screens that can showcase all kinds of content. Some cars are even capable of driving themselves, though this is a technology that's still developing. The concept, however, is that connected technology is fueling future transportation initiatives. It's thought that in the future, this will be a major part of the automobile industry.

Technically, smart technology in cars has been being used since 1996. Every single car that has been manufactured since has a built-in on-board diagnostic system. This helps mechanics understand some of the intricacies of vehicles by accessing data stored by the computerized system. You may have even used some of these diagnostic tools yourself when you see your Check Engine light turn on.

Some smart enhancements go beyond the practicality of diagnostics and simply make the user experience better…

Read the Rest Online!
https://dti.io/smarttech

How to Calculate if That Print Job Was Really Worth It

There are a few sounds that are familiar to any office: keys clacking away, coffee being sipped (or slurped), and the rattling, squawking hum of the printer. Yet this image presents a crucial question: do you know how much your printer is costing your business each time it is used? In today's blog, we'll review how you can calculate this investment.

Why Cost-Per-Page is So Important

It is pretty common knowledge in the business world that, in order for a printer to properly print, it needs to have ink with which to print. This ink comes in the form of ink cartridges, which need to be replaced once the ink within them has been spent. These cartridges are, unfortunately, anything but cheap - and you usually have to purchase multiple to get the full benefits of a multicolor printer.

This is part of the reason that it is important for you to know your printer's average cost-per-page (CPP), or at least have a figure that is reasonably close. If your business relies heavily on paper documents in its daily processes, these costs can be considerable.

How to Calculate the Average Cost-Per-Page

Despite different ink cartridges being made for a variety of different printers, the calculation to determine your CPP is relatively simple. All you have to do is divide the price of the cartridge by the cartridge yield rating, or how many pages the cartridge should be expected to print. This number can be found on the cartridge's packaging.

So, if you spent $25 on a cartridge of black ink with a yield of 525 pages, your formula would look like this...

$25/525 = 0.048$

...giving you a cost of about 5 cents per page.

Calculating CCP in More Complicated Printers

The fact that not all ink cartridges are the same can add a step or two to this calculation. Since many modern printers now rely on different cartridge configurations, like an individual cartridge for each color (black, cyan, yellow, and magenta) or two cartridges that cover them all (black, and cyan, yellow, magenta).

Regardless, your calculation will be more or less the same, with minor adjustments to account for how the colors are clustered or divided. Basically, when adding color into the equation, find the CPP of each color and combine your totals - including black. It is important to remember that when printing something in color, you're apt to use just as much, if not more, black ink as well.

Furthermore, it is important to consider that ink cartridge manufacturers will often base their yield rating on standardized business documents, with a certain percentage of the document being covered in ink. Therefore, printing something that doesn't fit into these constraints will throw off the yield, which can happen based on what kind of document you are printing, and even what kind of paper you're using...

Read the Rest Online!
https://dti.io/printjob
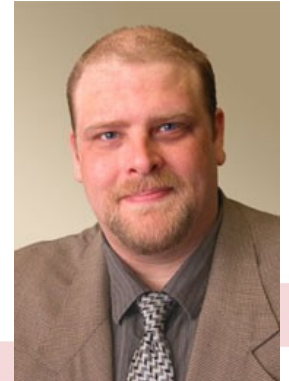
Chris Chase
Solutions Integrator
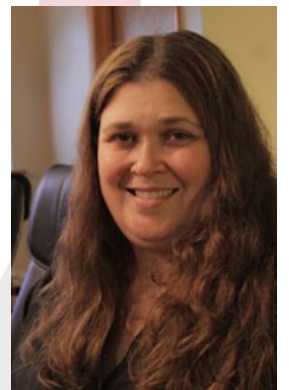
Charlotte Chase
Solutions Integrator

Directive

330 Pony Farm Road
Suite #3
Oneonta, NY 13820
Toll-Free 888-546-4384
Voice: 607-433-2200

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

newsletter@directive.com

facebook.directive.com

linkedin.directive.com

twitter.directive.com

blog.directive.com

instagram.directive.com