directive

TECHMinutes

October 2018

Your Small Business Technology Information Source!

This Issue:

Smaller Practices are Choosing Cloud-Based EHR

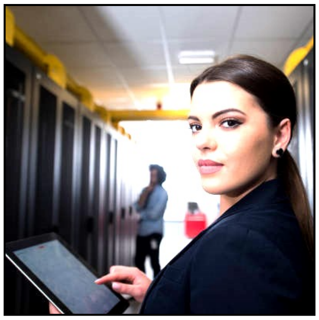
The medical field has spawned all kinds of new technology that takes patient care to the next level. Regulations demand that even smaller practices need to make the jump to electronic medical record systems (also known as electronic health records). These EMR/EHR solutions provide an interface that give providers and patients a way to keep themselves connected to each other--a tool to promote a more efficient delivery method for these services. We'll take a look at these EMR and EHR solutions that are hosted in the cloud, giving your organization…

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

In October, we join IT professionals from all over the U.S. to celebrate National Cybersecurity Awareness Month.

In promoting the strategies and practices that individuals, businesses, and other organizations utilize to protect their interests from the ever-growing number of threats found on the Internet, we work to advance the pervasive protection of data and information systems.

If Productivity Is a Constant Battle, Consider Using Mercenaries



The business landscape can be unforgiving. It can be filled with landmines that slow progress to a crawl and blitzes that send your head spinning. If you were to compare the business world to history's great battles, technology solutions are a business' weapons. They are the tools used to make the everyday grind possible. The more advanced an army's technology, the bigger the edge they have over outfits that don't have that technology...as long as it works as intended.

In the information age, if an army doesn't have enough people to take advantage of their weaponry, they have two choices: They can choose to automate the use of those weapons or they can hire people to train their general soldiers and to ensure that they are working as intended. These outsourced soldiers are called mercenaries. They are the ones that are proficient with the weaponry and the tactics needed to be effective at war.

(Continued on page 2)

Data Security Issues of 2018

Each year there are changes that need to be made in the way that organizations manage their IT security. In 2017, ransomware burst on the scene in full force, and cyber security strategies reacted, coming up with fully managed security platform that remediate issues better, and cost organizations far more than they would have spent on IT security just a short time ago. In 2018, the same problems persist, while other developing technologies threaten the natural order of things. Today, we will look at how cybersecurity is being approached in 2018.

Oh, Well, Yeah...Ransomware is Still a Plague

If you were to be one of the unfortunate organizations to have to deal with a ransomware attack, you would be dealing with about as difficult a situation as you would as a business owner. If, for some reason you don't know what ransomware is, it is a computer virus that encrypts data and then demands ransom to unlock the data before it is deleted forever. In 2018, ransomware stepped up its game. In crippling the city of Atlanta's internal network with the SamSam ransomware, hackers upped the ante. The general strategy is not to pay hackers, but in the case of Atlanta, what could have been $52,000 has cost the taxpayers

(Continued on page 3)

"Computers are useless. They can only give you answers."
- Pablo Picasso

Disasters Aren't Always Caused By Disasters

Disasters are a very real possibility that businesses have to deal with, but not all disasters come in the form of a flood or fire. You can predict weather effects that can create problems for your business, like thunderstorms and ice storms that bring down power lines, but you can't possibly predict when and how your organization will suffer from a data loss incident. We'll discuss in-depth how your business can save itself the trouble of dealing with cyberattacks and user error--particularly in regard to data backup and disaster recovery.

Cyberattacks are Disasters, Too

Even if cyberattacks aren't your first thought when you think of a disaster, it doesn't change the fact that the end results are strikingly similar to those of a flood or fire. Your infrastructure could potentially be rendered unusable for an extended period of time. For example, if your office is hit by a flood, chances are that it will sustain considerable damage that will keep employees from working in it until arrangements have been made to clean it up. When your network is hit by a cyberattack, you can't let your employees on the network until it's secure. Otherwise, you could make an already big problem much, much worse.

Cyberattacks can happen for a variety of reasons, but the majority of the time, they will be caused by a combination of two things: poor user security practices, and poor network security management practices. The former is a little harder to address, but for your network, you should be using a comprehensive enterprise-network security solution designed to keep threats out of your network. This includes a firewall, along with a dedicated antivirus, spam blocking software, and even a content filter, all to take a preventative approach to your organization's network security.

End-Users Don't Help

Depending on how much they are trained in how to prevent disasters and secure your network, untrained users could become a major detriment to your organization's success and survivability. Let's imagine a scenario when your organization needs to take a data backup due to your solution not being automated (tape backup). If your employees are the ones setting the data backup, there is a chance that they could potentially forget to do so, or do so incorrectly.

Untrained users can also be a major problem for the health for your network. Since the untrained user may fall victim to social engineering scams or phishing attacks, having a strategy to provide comprehensive training to the people that utilize your organization's computing network will pay dividends by delivering less downtime and a more effective network for your business.

Through proper training your staff should be able to identify potential security risks to your network and respond in kind. Directive can help you secure your network on both a technical side and end-user side by providing security and data backup solutions designed to mitigate damage as a result of disasters. To learn more, each out to us at 607.433.2200.

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

If Productivity Is a Constant Battle, Consider Using Mercenaries

(Continued from page 1)

In the case of business technology, the outsourced IT technicians at Directive are mercenaries in our own right. We have the proficiencies needed to make your IT work the way you intend it to, while providing the expertise needed to provide your staff the support and training needed to ensure that they can stay productive.

If business is indeed looked on as war, there are three major battles that businesses have to win to maximize their operational effectiveness. To win these battles, a business' high command may be prudent to enlist the use of a mercenary force of outsourced IT professionals.

Battle #1: Downtime

Inefficiencies that happen in your business may be unavoidable, but interruptions can largely be eliminated. Downtime is likely the costliest part of any technology-related problem; and, as a result, anything you can do to keep downtime to a minimum will help your efforts. IT mercenaries can present a lot of value in the battle against downtime. First, they continuously monitor and manage your business' network, ensuring that any inefficiencies or threats are proactively eliminated.

Additionally, the IT mercenary comes with its own weapons. Not only do we leverage automated systems to ensure your network and infrastructure are comprehensively managed, we provide complete data backup and recovery services that protect all of your organization's data against loss. Our BDR frequently and reliably backs up all your relevant data both to a network attached device and to an offsite data center, providing complete data protection and powerful redundancy.

Battle #2: Technology Implementation

Another battle that IT mercenaries can help with is project fulfillment. Most businesses are looking for an edge, and a lot of time the better your...

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

Data Security Issues of 2018

(Continued from page 1)

upwards of $17 million to remedy; and, they didn't get much of the data back. That's exactly how devastating ransomware can be to any organization's network. In 2018, ransomware kept coming for businesses, and now, with ransomware now being deployed through Internet of things devices, the situation is getting worse and worse. This new deployment technique is a major problem. Since ransomware is typically allowed onto the network, not placed there through infiltration, it makes the threat one that is going to be here long after the calendar shifts to 2019.

Nefarious A.I. Threatens Businesses

For the past couple of years, security professionals have been utilizing deep learning computing systems to try and mitigate threats. This has led to a whole industry of A.I.-based network security being pushed to organizations. But like any other defensive weapon, it can eventually be developed as an offensive weapon. Hackers are now beginning to utilize these complex computing systems to create ingenious methods of deploying devastating malware. This could be the next step in the evolution of malware.

More dangerous than A.I. systems finding places to deploy malware are A.I. systems that create malware. Introduced in 2018, a malware called DeepLocker is an A.I.-powered malware that is carried along by applications and is just dormant code until it reaches a specific victim, who is identified through a series of factors (including facial recognition, geolocation, voice recognition, or specific data flow). Once the target has been acquired, DeepLocker launches its attack. IBM is on record stating that the malware is "almost impossible to reverse engineer." This doesn't bode well for security professionals going forward.

What Role Will the GDPR Actually Have?

Since going into effect in May, the European Union's General Data Protection Regulation (GDPR) has had a major...

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

Protect Your Business From Phishing Attacks

Spam is a major hindrance when running a business that relies on email, but it's easy to protect your employee's time from the average spam messages with the right technological support. Unfortunately, hackers have adapted to this change and made it more difficult to identify scam emails. More specifically, they have turned to customizing their spam messages to hit specific individuals within organizations.

These messages, called phishing attacks, are targeted attempts to coerce information from users. They are particularly dangerous due to the fact that messages are personalized to target specific users or businesses. Unlike spam, which is typically sent en masse because of how generic the messages are, phishing attacks can yield major results due to how convincing the messages can look. DarkReading covered the results of a study which found that 91 percent of cyberattacks are started by a phishing email, highlighting the importance of phishing attacks in the hacking community.

These results come from PhishMe, which also covered the reasons why phishing attacks were so effective against users. Here are the numbers:

- Curiosity: 13.7 percent
- Fear: 13.4 percent
- Urgency: 13.2 percent

If you think about it, these numbers and reasons make sense. Employees undergo a considerable amount of stress throughout the workday due to a variety of factors. Some might worry about their work performance suffering, while others might feel pressured to click on certain attachments because someone tells them that it's important enough. Some might just not think things through before clicking on unsolicited attachments or links, leading to the gate being opened for hackers. Therefore, it makes sense to address these concerns with your staff while training them to identify phishing attacks.

Ways to Fight Phishing Scams

If you're having trouble showcasing the importance of phishing scams, consider the following tips and tricks from Directive:

- **Undergo regular phishing scam training:** If you train your employees to identify phishing scams, they will be less likely to fall victim to them in the future.
- **Double-check any suspicious messages:** Messages that you think are phishing attacks should be directed to your IT department.
- **Never respond to urgent requests before following up:** If you get messages from someone internally urging you to make a wire transfer or do something suspicious, follow up with them in person if possible.
- **Reconsider best practices and workflows:** If something seems out of place or suspicious, fall back on best practices to guide you to the best possible outcome.

You want to protect your business from phishing scams and other threats and the technology professionals at Directive can help. To learn more, reach out to us at 607.433.2200.

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

Tech Term: Hacker

The term "hacker" is possibly one of the best-known technology-related terms there is, thanks to popular culture. Properties like *The Girl with the Dragon Tattoo* and the *Die Hard* franchise have given the layman a distinct impression of what a hacker is. Unfortunately, this impression isn't always accurate. Here, we'll discuss what real-life hackers are like, and the different varieties there are.

Defining Hackers

In broad terms, a hacker is an individual that uses their computing and programming skills, sometimes cooperatively with others like them, to identify and exploit gaps in the protocols that protect computer systems. Their actions after that point can be used to classify them further.

There are three main classifications, with subtypes to specify different types of hackers more specifically.

The Types of Hackers

Black Hat

Black hat hackers are the first kind that you probably think about, as they are the bad guys of the hacking spectrum. They are the ones who use their computer skills to entrap their victims and steal information for their own benefit, largely contributing to the public perception of hackers as a whole. If someone is a black hat hacker, their work is motivated by personal gains, tends to take effect at the expense of others, and is illegal.

White Hat

White hat hackers fall on the opposite side of the hacking spectrum, electing to use their skills to help businesses and other organizations keep their IT systems secure by seeking out weak points and vulnerabilities so that steps can be taken to fix these problems. White hat hackers also only operate by request - they will not hack your systems unless you ask them to try. In a way, if Directive were to run a penetration test on your business, we would be operating as white hat hackers.

Gray Hat

As their name would suggest, gray hat hackers are a combination of black hat and white hat. While they avoid being classified as black hat by not personally profiting from a hack, they also aren't white hat, as their hacks aren't done with the permission (or knowledge) of their target. The vulnerabilities they find will sometimes be reported to the hacked organization or distributed online for others to take advantage of.

Hacker Subtypes

Script Kiddies

These are the amateurs, the hackers that rely on pre-written code to launch basic attacks on their targets. Their motivation is often to attract attention or to impress others, with no appreciation for why the codes they leverage work and no desire to learn.

Blue Hat

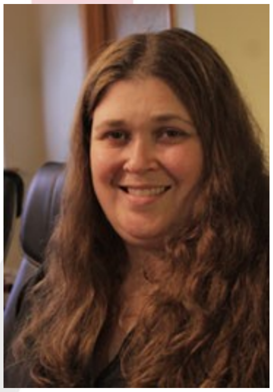
Similar to a script kiddie, a blue hat hacker is an amateur who uses the code written by others to lash out against those who have wronged them in their eyes. Again, like a script kiddie, a blue hat hacker has no desire to learn how hacking works, they just want to use it as a means to a vengeful end.

Red Hat

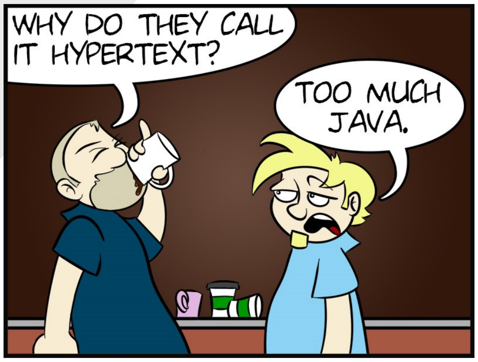
A red hat hacker is a hacker that targets other hackers. Rather than reporting a discovered attack, as a white hat hacker would, a red hat hacker will instead attack…

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

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