TECHNOLOGY TIMES

"Insider Tips To Make Your Business Run Faster, Easier And More Profitably"

What's New

Interested in a FREE YETI Tundra 105?

See page 2 for more information!

September 2017

This monthly publication provided courtesy of Rick Johnston, President of Information Management Systems

"Enabling People to Provide Great Products and Services - Anytime, Anyplace, Anywhere"

What Will You Do When This Disaster Hits Your Business?

WE PRACTICALLY GUARANTEE IT WILL HAPPEN TO YOU

In today' s world of rampant cybercrime, every savvy business owner knows the necessity of locking down their data. However, we find that the cyber security technologies used by the vast majority of businesses are woefully out of date. Sure, your current solution may have worked great, but digital threats to the safety of your company are constantly evolving. Criminals will eventually attempt to breach your data — and your barriers are not as secure as you might think.

Before World War II, the Germans developed a technology that would prove to be a key player in the conflict: its family of infamous Enigma machines. These devices, about the size of a small microwave, were composed primarily of a typewriter and a series of three or four rotors. By using a set of rules contained in a corresponding codebook, German soldiers would use the machine to encode vital messages to be sent covertly over the airwaves. The number of potential permutations — and thus solutions — for the code was in the tens of millions. The Germans were confident that the code could never be broken and used it for a vast array of top-secret communications.

The code's impenetrability didn't last. Via photographs of stolen Enigma operating manuals, the Polish Cipher Bureau reconstructed one of the stubborn Enigma machines, internal wiring and all, enabling them to decrypt the Wehrmacht's messages from 1933 to 1938. Facing an impending German invasion, Poland decided to share these secrets with the British. But, at the outbreak of the war, the Germans increased the security of the Enigma initiative by changing the cipher system daily. In response, a British code-breaking team, led by

genius English computer scientist Alan Turing, constructed primitive computers, known as "bombes," that allowed them to decrypt the incredibly complicated ciphers faster than ever before. But it wasn't until the capture of the U-110 warship and the seizure of its Enigma machine and codebooks that the British were able to decrypt the most complicated cipher of the war, the Kriegsmarine Enigma.

The information gleaned from these decrypts are believed to have shortened the war by more than two years, saving over 14 million lives.

Just like you, the Germans believed the systems they had put in place to defend their secrets were impenetrable. And it's true: the system had few cryptographic weaknesses. However, there were flaws in German procedure, mistakes made by Enigma operators, and failures to introduce changes into the Enigma formula — along with the Allied capture of key equipment and intelligence — that ultimately allowed the Allies to crack the code once and for all.

"TAKE THIS AS A CAUTIONARY TALE: the most advanced, complex cryptography system in the world became obsolete within 10 years. The same goes for your potentially outdated cyber security measures."

Take this as a cautionary tale: the most advanced, complex cryptography system in the world became obsolete within 10 years. The same goes for your potentially outdated cyber security measures.

Though they may not be led by Alan Turing and his crack team, you can bet criminals are constantly chipping away at the defenses of even the most powerful firewalls. The arms race between cyber security companies and cybercriminals rages on behind the scenes, and you can bet that they've already cracked your business's "Enigma." Just look at the massive European cyber attack this past June, which infected computers from over 27 companies across the continent, including those of the largest oil company in Russia, with ransomware. The unimaginable cost of that attack is something you certainly don't want your business to shoulder.

As technology evolves, so does crime. New threats arise each and every day. While solutions are available (and needed), they are notably absent in older software developed at a time before these constantly morphing attacks even existed.

Once the enemy has found a way to pick your lock, you need a new lock. Luckily, you have your trusty IT provider, constantly on the lookout for cutting-edge solutions that protect our clients from even the nastiest malware.

Don't be like the Germans. Constantly look at options to upgrade to more robust, better cyber security to defend yourself from the bleeding-edge hackers, and sleep safe knowing your business is secure. Education is the best way to familiarize your employees so your business doesn't fall to hackers. For a small monthly fee you can train your staff on the latest attacks and protect your network. Contact us today at 701-364-2718 or info@imsnetworking.com.

Do you want this YETI Tundra?

We love having you as a customer and, quite honestly, wish we had more like you! So instead of just wishing, we've decided to hold a special "refer a friend" event during the summer.

Simply refer any company with 10 or more users to our office. We will call and schedule an appointment. When we get the appointment we will send you a YETI Tumbler. If the referral you submitted becomes a client, you will receive a YETI Tundra 105 ($479.99 value!).

To submit a referral please go to: http://www.imsnetworking.com/about-us/referral-program/ or email info@imsnetworking.com

Shiny New Gadget Of The Month:

Building A Smarter Shower

The cutting-edge U by Moen Smart Shower is looking to revolutionize your shower experience. With digital valves and a corresponding controller, the U by Moen can make any shower a lot smarter.

After users install the digital valves and controller — a task that takes a few tools and a little bit of handiwork — the U by Moen allows them to sync their showers with their smartphone. The system then makes it easy to customize the showering experience, choosing the perfect temperature and saving preferences for future use. Start the shower remotely, and it will let you know when it's ready, automatically shutting off until you step in. Available for showers with either two or four outlets, the U by Moen is the perfect addition for those looking to digitize every aspect of their home.

Even After Wanncry, Many Companies Are Still Ignoring Network Security

Remember the global Wannacry ransomware attack? Remember the even more recent Petya attacks?

You would think after either of these, IT professionals around the world would have stepped up and immediately implemented better, stronger and more robust security protocols, because as those attacks proved, if the hackers want to, they can bring not just individual companies, but whole industries to their knees. That's the kind of warning it just doesn't pay to ignore, and yet, that's exactly what seems to be happening.

According to new research published by Tripwire, even in the face of the recent global attacks, more than two thirds of industry data security professionals do not feel that their organizations have made the necessary improvements to guard against such attacks in the future. Here's what the security professionals surveyed outlined as the biggest organizational challenges:

• 32 percent of respondents said their companies struggled even to know what devices were being connected to their networks

• 14 percent cited a lack of vulnerability management

• Six percent identified administrative privilege issues as being the main cause for concern

• And another six percent identified audit log attention as being the biggest point of weakness

You'll almost certainly note that those numbers do not add up to 100 percent. That's because the rest of the survey respondents indicated that there was no single point of identifiable weakness, but rather, that businesses were failing at all of the above.

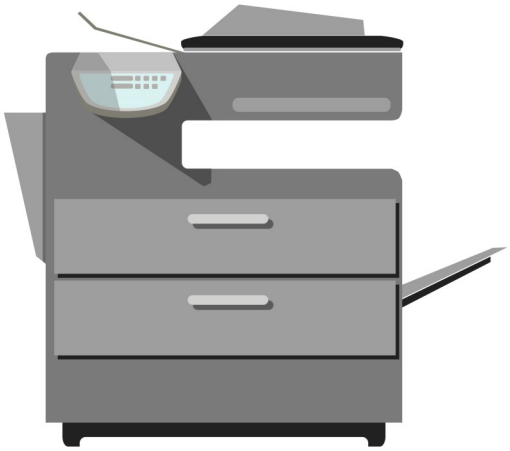
Bear in mind that the average cost of a successful data breach is now $7.5 million, up five percent from just last year, and that's before considering the costs of paying any ransom demanded by malware such as Locky-Diablo6, Wannacry and Petya, and yet, in spite of this, few companies are making any serious moves to improve their data security.

Don't let your company fall into that trap. If your security isn't as robust as you think it could be, take steps immediately. Failing to act makes your firm a ticking time bomb. It's not a question of if the hackers will come for you, it's a question of when.

Bits & Bytes

Your Copier Is Spying On You

It may sound paranoid, but it's true: the machines you use every day around the office could be spying on your data. Copiers and multifunction printers, particularly, are some of the



leading causes of business data breaches. When you consider it, it makes sense. They're among the only devices on the network that rarely have their default password changed. But these advanced copiers and printers often house images of all the pages they've ever scanned on an internal hard drive, making them the perfect target for thieves. Make sure to change the password from the default on every network-connected device in your office. This one simple step can save you a costly headache down the road. *intellisystems.com 01/31/2017*

Your Best Employee WILL Quit … Are You Prepared?

Employee churn is a fact of business. It's important to take steps to ensure that regardless of an employee's importance, their loss won't be catastrophic. Consider everyone on your team. If they left, what would it do to your business? Make sure to document indispensable knowledge. In the end, you should keep your team as happy as possible, but be supportive if they make the decision to leave. *Groovehq.com 12/10/15*

Fight Traffic Tickets WITHOUT Leaving the Comforts of Home

"Off the Record" is a new app that allows you to contest those pesky speeding tickets without ever leaving your house. All you have to do is take a picture of your ticket, answer a couple questions, and pay a fee (ranging from $53 to $599, depending on your area). The app will then assign the case to a local lawyer to contest the charge. It may sound too good to be true, until you consider its 97% success rate. Best of all, if the ticket is not dismissed, deferred, or reduced to a nonmoving violation, you'll get a full refund! *lifehacker.com 7/7/17*

If you work at a standing desk, you'll love this.

Ergonomic experts agree that "your best position is your next position." In other words, your body is meant to move. And constant motion reduces fatigue as well as back and joint pain. Enter the Wurf Board, an inflatable platform for working at a standing desk. As you stand on it, your body constantly adjusts, keeping you in a subtle state of constant motion. Benefits include greater energy, focus and calorie burn. While anti-fatigue mats make standing comfortable for an hour or so, the Wurf Board lets you stand easily for hours at a time. Priced at $199-$269 and available in three sizes, it lets you work out while you work. *-TheBalance.com*