# TECHNOLOGY TIMES

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

## What's New

Rick is going to speak at the ND Rural Water Users Association about Cyber Security and securing SCADA Systems this month.

Previously he has spoken to the North East Dental Association about Security Threats.

If your organization is interested in having Rick speak about Cyber Security or other IT related topics contact us today—info@imsnetworking.com or call 701-364-2718.

## February 2018

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

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

# WARNING: Your Business Is More Likely To Be The Victim Of Cybercrime NOW Than Ever Before…Take These Steps Today So You Don't Get Hacked!

Though we're in the midst of an unprecedented rise in high-profile cybercrime incidents, it's easy to assume that our own much smaller businesses are safe. Sure, we think, hacking into the data stores of J.P. Morgan, the U.S. Government, or Virgin America can net hackers millions and millions of dollars. Why would they bother with a small business?

But unfortunately for all of us, hackers actually *do* bother with small businesses across the country — these attacks just don't make the news. By some estimates, including one reported in Media Planet, more than half of small businesses have had their data compromised. According to StaySafeOnline.org, these attacks, targeting small to midsize companies, now comprise over 70% of all data breaches. What's worse, this digital onslaught shows no sign of slowing. In fact, ransomware attacks alone have increased 250% since 2016, accompanied by higher rates of malware, phishing, and other forms of cybercrime.

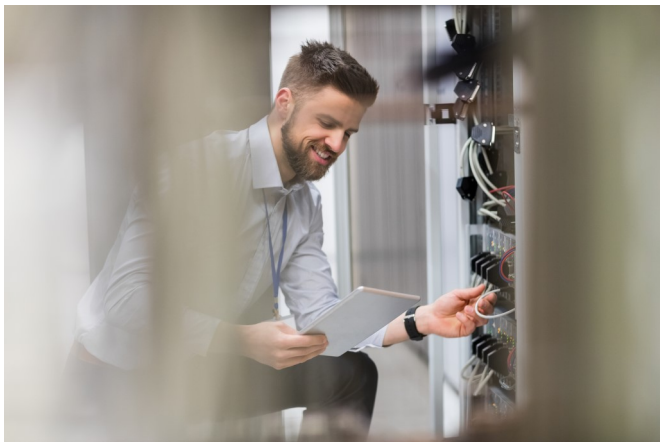
Once you see these numbers, it's easy to understand why hackers

seek the little guy. These days, massive corporations like Google or Citigroup employ incredibly sophisticated digital measures. Their digital vaults, though containing ludicrously attractive sums of potential money to grab, are located at the end of a virtual labyrinth covered in traps, with a final, inches-thick steel door protecting their assets for good measure. In contrast, the digital assets of small businesses are often hidden behind nothing more than a single, often weak, password. With thousands of business owners going about their day-to-day, utterly oblivious to their paper-thin security, the question turns from "Why would hackers bother with my small business?" to "Why *wouldn't* they?"

Though cybercriminals may come away with less than they might have had they targeted a Fortune 500 company, it certainly isn't going to seem cheap to you. According to one TechRepublic analysis, an average cyber-attack on a small business can cost as much as $256,000. Is that a sudden cost your company can weather?

Luckily, there is hope. Though small business owners often assume that effective cyber security solutions lie far outside their budget range, robust digital security is now more affordable than ever. By investing in comprehensive protection, small businesses can deflect even the most persistent hackers.

> **"What's worse, this digital onslaught shows no sign of slowing. In fact, ransomware attacks alone have increased 250% since 2016, accompanied by higher rates of malware, phishing, and other forms of cybercrime."**

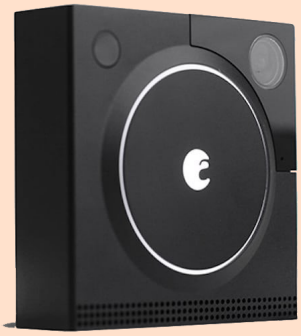


Today, a cyber-attack on your business is almost statistically inevitable. And when that attack comes, you'll definitely want to be prepared. If you haven't needed a doctor for the past two years, does that mean you're going to abandon your health insurance coverage? Of course not. What about car insurance? Does it become unnecessary in the absence of a crash? No, because even if you're the best driver in the world, sometimes a collision is out of your control.

What's more, both your body and your car require regular upkeep and maintenance to remain in peak condition. It's no different with your network security. As technology hurdles forward at an ever-increasing speed, the ways that hackers can infiltrate your network multiply. The best digital security platforms constantly update, enabling them to anticipate these shifts and prevent them from becoming liabilities. This way, you can be proactive prior to a digital crisis, ensuring that no matter what comes, your network is protected.

Even as digital crime climbs at a staggering rate, and hundreds of small businesses are forced to close their doors for good, thousands of owners fail to notice, assuming they'll somehow be spared from an attack. Don't be one of them. Invest in regularly maintained, powerful cyber security, and ensure the future of your company.

## Shiny New Gadget Of The Month:



### August Doorbell Cam Pro

It's 3 a.m. You and your family are all tucked away in your beds, snoozing away. Suddenly, the doorbell rings, and everyone is shocked awake. Who is that? What do they want? And, most importantly, what should you do?

It's a dicey situation, but luckily, modern technology has an answer — the August Doorbell Cam Pro. Another addition to the endless list of "smart home" offerings, the device is a small, unassuming square doorbell. At any time — say, when a dark figure is looming on your porch in the middle of the night — you can open up your phone and take a look through the August Doorbell's camera. After that, if you feel like a conversation is in order, you can talk through the device's built-in microphone and speakers. With the ability to sync up to August's smart locks and Amazon's Alexa, the August Doorbell Cam Pro is a vital and convenient security addition to any smart home. cnbc.com

# Know the Risks of Amazon Alexa and Google Home

Voice-activated, internet-connected personal assistants are all the rage these days. Ask a group of friends what they got for Christmas and at least one will tell you how much they love their new Amazon Echo, Google Home or some equivalent.

This piece of smart home technology is a beautiful thing. But like all good things, there are risks.

Your technology is listening.

The main concern among security experts when it comes to smart home devices is the degree to which they are listening. They obviously listen for any commands the user might utter, but what else is it taking in, and how could that put privacy at risk?

Personal assistants fit into the larger concept of the smart home, so it's useful to look at threats that have already targeted Internet of Things (IoT) devices.

Security experts have long predicted threats targeting everyday home devices connected to the internet, and the threat was made plain last fall when Mirai malware was used to hijack internet-facing webcams and other devices into massive botnets that were then used to launch a coordinated assault against Dyn, one of several companies hosting the the Domain Name System (DNS). That attack crippled such major sites as Twitter, Paypal, Netflix and Reddit.

To be clear, that attack infected IoT devices and used them to target a company. It's not the same as being snooped on, but in many cases the end goal is on the same wavelength: the bad guys want to see or hear what you have for personal data so they can use the information to benefit themselves or their cause.

Defensive measures

Those who choose to use this technology can't and shouldn't expect 100% privacy. If not for the ability of Amazon Echo and Google Home to listen, these things would become nothing more than doorstoppers and paperweights.

But there are certainly things users can do to limit the risk of unintended consequences. Here are just a few examples:

•Not currently using your Echo? Mute it the mute/unmute button is right on top of the device. The "always listening" microphone will shut off until you're ready to turn it back on.

•Don't connect sensitive accounts to Echo On more than a few occasions, daisy chaining multiple accounts together has ended in tears for the user.

•Erase old recordings If you use an Echo, then surely you have an Amazon account. If you go on Amazon's website and look under "Manage my device" there's a handy dashboard where you can delete individual queries or clear the entire search history.

# Bits & Bytes

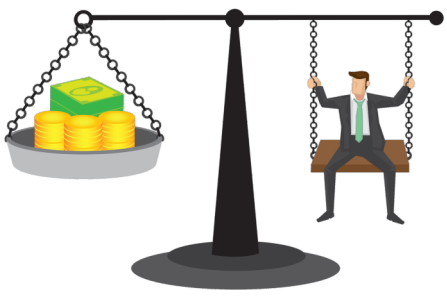
## Drop These 4 Habits For A Successful 2018

Today, the business world is more rapid, complex, and volatile than ever before in history, a trend that shows no signs of slowing down. With that in mind, it's vital that entrepreneurs tighten up their business practices now, not later.

Here are four bad habits to kick in order to shed your company's sluggishness and step fully into the modern marketplace:

**1.** Procrastinating training investment: Investing in comprehensive training resources, which expands the skills of both you and your employees, can ensure you stay competitive in the midst of constant change.

**2.** Amassing knowledge without applying it: With millions of well-meaning advice articles plastered across the Internet, it's easier than ever to learn new principles. But you can't stop there. Actively implement the knowledge you gain, instead of keeping it locked away in your mind.



**3.** Expecting ideas to come from the top down: Today's savvy business owner doesn't solely channel those at the top of the organization chart. Instead, they welcome ideas from all levels of the company.

**4.** Busywork: Too many leaders get caught up in output metrics instead of outcomes. Get the numbers out of the way and watch your employees shine.
*Inc.com 11/16/2017*

## How To Spot A Phishing E-mail BEFORE It Can Do Any Damage

Phishing e-mails are bogus messages carefully designed to look like a legitimate message (or attached file) from a site or person you trust. Their goal is getting you to willingly give up your login info or unknowingly click a link to install a virus. The best of these e-mails look uncannily similar to their real-world counterparts, but there are ways to discern a phishing attempt from a legitimate e-mail.

First, hover over — but don't click on — the URL in the e-mail to see the actual website you'll be directed to. If there's a mismatched or suspicious URL, delete the e-mail immediately. Other telltale signs are poor grammar or spelling errors. And if the e-mail asks you to verify or validate your login or personal information, get out of there.

## 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.