progressive computing

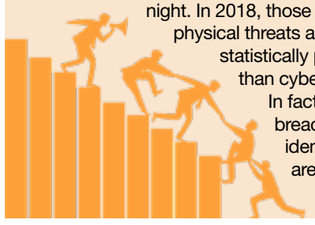
35 East Grassy Sprain Road
Yonkers, NY 10710

Inside This Issue

The "Not Me!" Problem...And Why This Is Almost Guaranteed TO Happen To You

Security this, password that – now they want a password with 14 characters with two symbols? And I have to change it every three months? As difficult as it is to remember 24 different passwords, four PIN numbers and a slew of new cyber security processes, we still manage to instantly recall most of the tangible things in our lives. The code for the company door and alarm system, the passcode to our phones, the garage code, the other garage code – you get the idea.

But these numbers are based upon a time when the most "real" threat seemed to be someone busting in our door and threatening our families in the middle of the night. In 2018, those kinds of physical threats are far less statistically prevalent than cybercrime. In fact, data breaches and identity theft are occurring at three times the rate that home burglaries occur in the U.S. according to a 2016 study by the University of Kentucky.



Don't succumb to the "Not me!" approach to the shift in crime. Understand that it can happen to you, and approach all aspects of physical and electronic security with the attention they deserve.

7 Things Mentally Strong Leaders Never Do

Leaders need to stay mentally sharp to effectively lead their teams. Here are seven things that truly strong leaders never, ever do.

1. They don't mask their insecurities, but instead maintain their humility and acknowledge their mistakes and weaknesses.
2. They don't go overboard with their emotions. Instead of suppressing their feelings, real leaders stay aware of how their emotions influence their behavior.
3. They accept criticism with open arms. Instead of protecting a fragile ego, mentally strong leaders take unfavorable feedback and use it to improve their processes.
4. They take responsibility for their actions. When a good CEO messes up, they apologize with sincerity and accept the consequences of their behavior.
5. They don't mistake kindness for weakness. Offering extended bereavement leave isn't letting your employees take advantage of you – it's a common courtesy.
6. They don't confuse confidence with arrogance. Though they're sure of themselves, a good leader recognizes the necessity and competence of their team. They don't put themselves over others.
7. They don't fear other people's success. When someone else is doing great things, they know that it doesn't diminish their own accomplishments.

Inc.com 12/12/2017

progressive computing

THE PROGRESS REPORT

Everything you need to know in a few minutes or less...

646-760-2071 • www.progressivecomputing.com

What's New?

We had an amazing time as a sponsor of the Kestra Ascend conference in Dallas. We met with hundreds of wealth advisors from across the county to discuss their IT needs and cyber security best practices. We offered a free dark web scan for all attendees. This scan identifies if a company's digital credentials are for sale on the dark web. We have scanned our Partners too, and will be reaching out with the results.

March 2018

This monthly publication provided courtesy of Robert Cioffi.

Our Mission:

We believe that our partners deserve the best possible service and support. We strive daily to improve our systems, processes and procedures to ensure that we can make a lasting relationship. Please don't hesitate to reach out if you have any questions or concerns about the service we provide.

5 Ways Your Employees Will Invite Hackers Into Your Network

Whether they're criminals or heroes, hackers in the movies are always portrayed as a glamorous group. When it comes down to the wire, these are the individuals who crack into the ominous megacorporation or hostile foreign government database, hitting the right key just in the nick of time. They either save the day or bring down regimes, empty the digital vault of the Federal Reserve or disable all the power plants in the country. It's always a genius up against an impenetrable fortress of digital security, but no matter what, they always come out on top.

In real life, it's rarely that difficult. Sure, if you look at the news, you might believe hackers are close to their Hollywood counterparts, stealing data from the NSA and nabbing millions of customer records from Equifax. But the majority of hacks aren't against the big dogs; they're against small to mid-sized businesses. And usually, this doesn't involve actually hacking into anything. A lot of the time – approximately 60% according to the *Harvard Business Review* – an unwitting employee accidentally leaves the digital front door open.

The biggest threats to your company aren't teams of roaming hackers; they're your employees. Here's why.

continued on page 2

...continued from cover

1 They'll slip up because they don't know any better.

With the proliferation of technology has come an exponential rise in digital threats of such variety and complexity that it'd be impossible for the average person to keep track of it all. Each of your employees' lives are a labyrinth of passwords, interconnected online accounts and precious data. If their vigilance slacks at any point, it not only leaves them vulnerable, but it leaves your company vulnerable as well. For this reason, most cyber-attacks come down to a lack of cyber security education.

> **"It's a sad fact that a huge portion of digital attacks are the result of company insiders exposing data... [b]ut there is one way you can make a concrete change that will tighten up your security more than you realize: educating your people."**

2 They'll let you get hacked on purpose.

It's a sad fact that a huge portion of digital attacks are the result of company insiders exposing data to malicious groups. Whether it's info vital for your competitive advantage, passwords they can sell to hacker networks to make a quick buck or sensitive data they can make public simply to spite your organization, it's difficult to protect against a double agent.

3 They'll trust the wrong person.

For many hacks, little code is needed whatsoever. Instead, hackers are notorious for posing as a trusted member of your own team. And if you believe that you'd be able to spot an impostor from a mile away, you may want to think again. Not only is it easier than ever to crack individual users' e-mail passwords and login credentials, and personal info is now littered throughout social media. A simple visit to Facebook can give a hacker all they need to know to "social hack" their way into the heart of your business.

4 They'll miss red flags while surfing the web.

Clickbait is more than a nuisance plaguing your social media feeds. It can be a powerful tool for hackers trolling for easy prey. If an employee doesn't understand what exactly makes a site or link look dubious, they may open themselves – and your company – to browser exploits or other types of attacks.

5 They're terrible at passwords.

According to Entreprenuer.com, "3 out of 4 consumers use duplicate passwords, many of which have not been changed in five years or more." Even more of those passwords are simply weak, inviting easy access for unsavory elements. Many people brush off the importance of strong passwords, but the risks posed by the password "123456" or "password" cannot be overstated.

When it comes to defending your precious assets against digital threats, it can seem impossible to protect yourself at every turn. But there is one way you can make a concrete change that will tighten up your security more than you realize: educating your people. Through a comprehensive security training program, including specific examples of methods hackers use – particularly phishing – you can drastically minimize the risk of an employee accidentally opening up a malicious e-mail or posting sensitive info. When you make a concerted effort to make the entire organization vigilant against cyber-attacks, you're much less likely to be targeted.

Free Report: What Every Small-Business Owner Must Know About Protecting And Preserving Their Company's Critical Data And Computer Systems

This report will outline in plain nontechnical English common mistakes that many small-business owners make with their computer networks that cost them thousands in lost sales, productivity and computer repair bills, as well as providing an easy, proven way to reduce or completely eliminate the financial expense and frustration caused by these oversights.

Download your FREE copy today at www.progressivecomputing.com/itsecurity or call our office at 646-760-2071.

Cartoon Of The Month

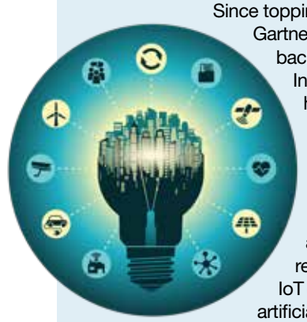
"Here's what you're going to do. You're going to give those 3 million people their credit card numbers back and you're going to say you're sorry."

SHINY NEW GADGET OF THE MONTH: FIXD

When was the last time you turned on your car, pulled out of the driveway and suddenly noticed the engine light pop up on your dashboard? You probably just ignored it and drove to your destination. Maybe the next day you spent some time trying to get to the bottom of the issue, only to come up short. Everything seems fine, so what's going on?

A new device called FIXD aims to figure that out. After plugging in the $59, palm-sized widget into your car's onboard diagnostics port – the same one mechanics use to find potential issues – it can communicate with a free app to tell you precisely what's wrong with your vehicle. You can determine why your engine light is on, how serious the problem is, and whether it requires emergency repairs, all without risking being ripped off by shady mechanics. If necessary, the device can actually turn off your engine light right from the app, making it a nuisance of the past.

How The Internet Of Things Is Changing Business



Since topping the list of Gartner's Hype Cycle back in 2014, the Internet of Things has risen to the top of business leaders' attention across the country. In fact, according to a report by *Forbes*, IoT outranks artificial intelligence, robotics and numerous other technological concerns as "the most important technology initiative by senior executives." As more companies leverage IoT tech, it's quickly becoming the next big thing businesses must keep an eye on to maintain their competitive advantage. As IoT continues to grow, those that fail to adopt these new opportunities may be left in the dust.

Cash In On Your Million-Dollar Idea

So, you came up with a brilliant idea. A million-dollar idea, even! But right now, that's all it is. The question is, how do you turn that big concept into cold, hard cash?

1. Write it down. How many light-bulb moments do you have at 2:00 a.m. and then forget come 9? Or, worried that your idea will be stolen, you keep it to yourself, promising to chase it down when you finally get the time. If you actually write down every money-making scheme you think up, one of them is bound to be the real deal eventually.

2. Once you settle on the idea you want to pursue, write a pros-and-cons list. What could make your idea truly successful? What could make it a total bust? Once you identify the cons – a too-high initial production cost or a newcomer in a competitive industry – you can start your search for solutions.

3. Determine your audience. Who do you think will buy your product or service? Run business surveys to determine whether there's a market for what you want to sell.

4. Figure out what problem you're solving. Uber eliminated the inconvenience of hailing a taxi and the difficulty of pre-ordering a ride, all for an affordable rate. Apple lowered the cost of technology and made it user-friendly at a time when computers were designed for engineers and tech professionals. If you solve a real problem that exists in the market, consumers won't be able to live without your product.

5. Find a business partner. Although you may want to keep your idea to yourself, remember that it takes two flints to make a fire. How many successful start-ups do you know that were founded by a single person?

6. Start to think about money. If you don't already have some rainy-day funds to dive into, consider crowdfunding, borrowing from friends, credit cards or loans. Know the risks you're taking before moving forward.

7. Create a financial model. If you want to attract investors, a financial model that forecasts the fiscal performance of your business will show them your expected profitability and their return on investment. This makes you a more reliable bet.

8. Develop your prototype or beta test. This will allow you to see if your idea will actually work in the real world.

9. Prepare to be flexible and roll with the punches. Odds are, your initial idea won't be the same as your final product, and that's okay.

10. Keep on the sunny side. There are going to be truckloads of people who try to tear you and your idea down on your road to success. Stick to your guns – it's your baby and your investment of time and money, so make sure you believe in it.

MIKE MICHALOWICZ (pronounced mi-KAL-o-wits) started his first business at the age of 24, moving his young family to the only safe place he could afford – a retirement building. With no experience, no contacts and no savings, he systematically bootstrapped a multimillion-dollar business. Then he did it again. And again. Now he is doing it for other entrepreneurs. Mike is the CEO of Provendus Group, a consulting firm that ignites explosive growth in companies that have plateaued; a former small-business columnist for The Wall Street Journal*; MSNBC's business makeover expert; a keynote speaker on entrepreneurship; and the author of the cult classic book* The Toilet Paper Entrepreneur. *His newest book,* The Pumpkin Plan, *has already been called "the next E-Myth!" For more information, visit www.mikemichalowicz.com.*