

THE TECHNOLOGY TIMES NEWSLETTER

Cybercriminals Now Have a Bull's-Eye on Small Business...Is Your Company's Data at Risk?

In a December 2014 survey by the National Small Business Association, 61% of small businesses reported being victims of a cybercrime within the past 12 months.

The average cost to recover from a cyber-attack skyrocketed from \$8,699 per attack in 2013 to \$20,752 per attack in 2014. And, of the businesses targeted, 68% said they'd been hacked more than once.

Experts agree, as cybercrooks become ever more sophisticated, the threat to small businesses is going to get worse before it gets better...

So what can you do to beat the bad guys?

Here are three common ploys used by hackers – and how you can fend them off:

Phishing – A really legitimate-looking e-mail urges you to click a link or open a file that triggers a malware installation on your computer.



Best Defense: Don't let anyone in your company open files or click links in an e-mail unless they're certain who it came from.

Cracking Your Password – Hackers can run programs 24/7 testing password combinations. The easier your password is to guess, the more likely it is they'll crack it.



Best Defense: Consider using a password manager that generates and stores tough-to-crack passwords. For extra security, use unique passphrases for financial accounts in case the manager gets hacked.

Drive-By Download – You visit what appears to be an innocent site; yet when you click, your device gets hacked – and you may never know it, until it's too late.



Best Defense: Make sure your browser is up-to-date, or use one that updates automatically, such as Firefox or Chrome. Internet Explorer users have been found to be most vulnerable to these attacks.

Unfortunately, these three examples are just a small sampling of the dozens of ever more ingenious ways cybercriminals are breaking down the doors and destroying unprepared businesses.

Let us help! Through September 30, call our office at (212)235-0260 and receive a **FREE 15-Point Cyber-Security Audit** to uncover gaps in your company's online security.



"As a business owner, you don't have time to waste on technical and operational issues. That's where we shine! Call us and put an end to your IT problems finally and forever!"

Howard Globus,
IT On Demand

**Providing Excellent Support to the
New York City Area**

Inside This Issue...

Page 1 Cybercriminals & Small Business

Page 2 Cybersecurity: The Low down

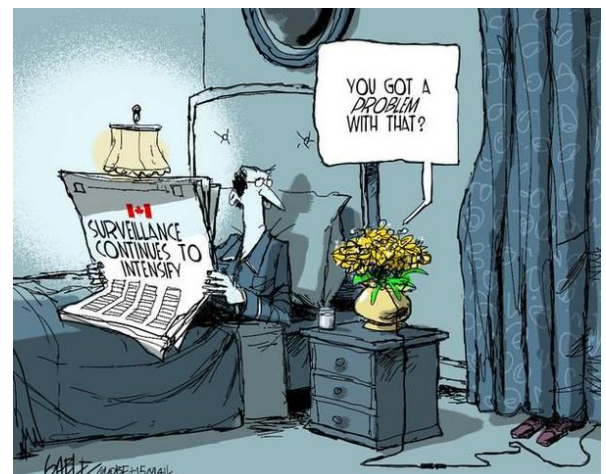
Page 2 Is Your Business Prepared for a Disaster? Let Us Help!

Page 3 New Gadget of the Month

Page 3 "Turn Your Biggest Weakness Into Your Greatest Strength"

Page 4 Do You Accept Credit Cards? Watch Out for these 5 Pitfalls!

Page 4 IT Fun Facts



Cybersecurity: The Lowdown on the Uptick

When it comes to cybersecurity, it's no secret that business is booming. Industry reports show job postings for cybersecurity professionals have increased 74 percent in the last five years, and hundreds of thousands of positions now exist. But what does this growth mean for *your* business?

As the demand explodes, the industry is struggling to keep up, and as a result businesses may be paying for IT professionals that can't adequately meet their security needs. ISACA recently published a study entitled "The State of Cybersecurity: Implications for 2015," which surveyed 649 cybersecurity and IT firms globally. Among its findings was the sobering statistic that as little as one fourth of those applying for jobs related to cybersecurity in the last year possessed the required skills for the position.

And security needs are certainly increasing. High profile breaches like those of Target and Home Depot in 2014 highlight the recent surge in cyber crime. According to the Global State of Information Security Survey 2015, conducted by PwC, cyber attacks have increased in frequency by 48% in 2014 alone. Incidents now occur an average of 117,339 times per day around the world.

The good news? The high demand can also attract talent, with many drawn to the promise of better salaries and job security. For those that *are* skilled and competent, the field of cybersecurity is a rewarding one.

Need some help navigating your own cybersecurity needs? Contact us at (212)235-0260 or email us at info@it-on-demand.com. We're proud to offer experienced, capable assistance that will help protect your business.

Our Disaster Recovery Plan Goes Something Like This...



Do You Have A Disaster Recovery Plan Like Dilbert's?

Let's face it: no one likes to think about bad things happening to them, much less plan for them. But since September is National Disaster Preparedness Month, **we want to offer you a FREE Disaster Recovery Assessment to get answers to these CRITICAL questions:**

- * How fast could you realistically be back up and running in the event of any natural or human disaster?
- * What backup, security and business continuity systems do you currently have in place, and are they sufficient?
- * Is all of your critical data being backed up, every day?
- * What are the largest threats to the security and integrity of your critical business data?
- * Do you know what steps and costs would be involved to rebuild your server and recover your data if you had to?

Claim Your Free Assessment now by visiting:
www.it-on-demand.com/disaster-recovery/

Shiny New Gadget Of The Month:



Nest Cam: Keeping an Eye on Things While You're Away

Have you ever worried about what's happening at home when you're away? The Nest Cam can keep you informed. This wide-angle camera streams sound and video to your smartphone. It will even warn you about any unusual activity.

If the Nest Cam detects sudden movement or loud noises, it instantly alerts you by phone. The video feed lets you see what's happening and even scold kids, pets or burglars through a speaker.

This product integrates with other Nest equipment. For example, smart smoke alarms can activate the Nest Cam. It also saves alerts and footage in a convenient archive. The camera even makes it easy to share fun video clips online.

If you already have WiFi, setup is a breeze. This gadget comes with a stand that lets you put it on any flat surface. It also sticks to metal objects or screws onto a regular camera tripod.

How Great Leaders Inspire Their Employees To Higher Commitment And Performance

You know the standard approach – first, identify your company's weakness and then do everything you can to fix it. Practice at it relentlessly, feed your team (and yourself) with constant affirmations, do anything you can to dive deep into your weakness and fix it once and for all. If you can't fix it, then go to Plan B by burying the weakness in hopes that none of your prospects or competitors find out.

Well, here's the dealio: the business down the street that is naturally strong at the same thing your company is weak at is working just as relentlessly to improve their strength. While you are fixing something that's broke, they are getting better at something that already works. While you may improve your weakness, their strength gets better too. At the end of the day they are still ahead of you. You lose. That is, unless you know the power of spin.

Instead of trying to fix weaknesses, smart leaders will turn the tables and make their weakness or even an industry weakness a competitive advantage. A wonderful example in the restaurant industry is Dick's Last Resort. Like all restaurants that struggle with the occasional rude waiter, Dick's could have tried to fix this industry-wide weakness. Instead they turned the weakness into their greatest strength. Known to have the "most obnoxious waitstaff in the world," Dick's built a whole system around exploiting an industry weakness. They hire and train people to be obnoxious (while the competition tries to fix it), and Dick's has grown explosively.

I have found that exploiting a weakness can draw droves of prospects. So, let's do it with your weakness. Here are the three simple steps you need to take:

Step 1

Know what your (or your industry's) weakness is. The process is simple: ask your customer and prospects what they don't like about your industry. Ask more customers the same question. Very soon you will know exactly what weakness they see.

Step 2

Instead of brainstorming ways to fix it, brainstorm ways to make the weakness absurdly weak. Can you make fun of it? Can you make it the core experience for your customers (think Dick's Last Resort)? How can you make the weakness a good thing?

Step 3

Now that you have a new and improved weakness, let the world know all about it. Market it to your prospects, inform your customers and even leverage all that work your fiercest competitor put into highlighting your weakness in the past.

The process of spinning a weakness takes courage, and that is exactly why it works. It is likely you have been afraid of doing this in the past, and it is highly likely your competitors are just as afraid too. If you have the courage to spin your weakness into an über-weakness (a.k.a. a big-time strength), you might just blow your competition out of the water once and for all.



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 <http://www.mikemichalowicz.com/>.

Do You Accept Credit Cards? Watch Out For These 5 Pitfalls That Could Lead To Lawsuits

If your company is not fully compliant with Payment Card Industry (PCI) Security Standards, you could be at risk of a serious tangle with attorneys. Technically, PCI guidelines are not a hard-and-fast set of laws. However, merchants can still face hefty liabilities for not meeting them. Avoid these mistakes to keep your company out of hot water with attorneys:

1. Storing Cardholder Data In Noncompliant Programs

Many states have laws regarding data breaches and, depending on where you accept cards, you may be subject to many of them. For example, Massachusetts has 201 CMR 17.00, which requires companies keeping any personal data from Massachusetts residents to prepare a PCI-compliant plan to protect that data. If a company then fails to maintain that plan, the business may face state prosecution.

2. Fibbing On The Self-Assessment Questionnaire

If you have considered tampering with the reports from your company's Approved Scanning Vendor, think again. Time invested now to fix any holes in your data security system could save you big-time from the penalties your company could suffer if there's ever a data breach.

The same thing applies to simply "fudging the truth" on self-prepared compliance reports. Even if you think it's a harmless stretch of the truth, don't do it.

3. Not Using The Right Qualified Security Assessor

Many companies use Qualified Security Assessors to help them maintain their PCI compliance. Every QSA does not necessarily know as much as another, however. It's important to select someone who both understands your business and stays up-to-date on the latest version of PCI Security Standards.

4. Trying To Resolve Data Compromises Under The Radar

You may be tempted to fix a customer's complaint yourself if they inform you of a data compromise. Not informing credit card companies of data breaches, however small, can lead to you no longer having access to their services. Those credit card companies can then file suit against your company, costing you big bucks in the end.

5. Not Checking ID For Point-Of-Sale Credit Card Use

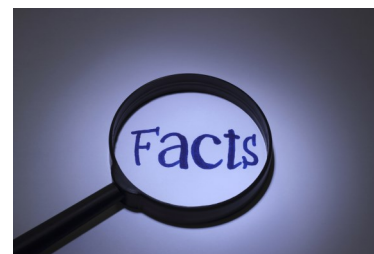
Sometimes it seems like no one checks IDs against the credit cards being used, so merchants tend to be lax about doing so. Unfortunately, running just one unauthorized credit card could cost you a lot in the long run.

Even if the state in which you do business does not have specific laws regarding PCI compliance, a civil suit may come against your company for any data breaches. The court will not favor you if you have not been PCI-compliant.

All in all, it pays to pay attention to PCI compliance – a little time invested today could save you big-time tomorrow.

The Lighter Side:

IT Fun Facts



Technology has forever changed our lives and our world more than you know. Here are some numbers to put that fact into perspective:

1. About 4 billion people worldwide own a mobile phone, but only 3.5 billion people own a toothbrush.
2. Computers and other electronics account for 220,000 tons of annual trash in the U.S. alone.
3. About 300 hours of video are uploaded to YouTube every minute.
4. Around 100 billion e-mails traverse the Internet every day, and about 95% of those messages go straight to spam folders.
5. The annual amount of electricity it takes for Google to handle a billion search queries every day is around 15 billion kWh, which is more than most countries consume.
6. About 500 new mobile games appear on the Apple App Store each day.
7. The "father of information theory," Claude Shannon, invented the digital circuit at age 21 while he was in college.
8. Regular computer users blink only half as often as non-users.
9. Over 1 million children can say their parents met on Match.com.

