TechTelegram
powered by neoRhino

What's New

If you're reading this, then odds are you have checked out our completely revamped and now mobile-friendly website. If you haven't, you should!

Our rhinos are working hard on providing informative and helpful content (including a new Blog page!) with a fresh, updated look to see what our company is all about.

Be sure to visit our social pages as well! Links are in the icons below.

August 2016

This monthly publication provided courtesy of Dave Pense, Network Engineer of neoRhino IT Solutions.

"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!"

Employees Keeping Your Data Safe? Don't Count On It

The biggest block to protecting your company's data is employee ignorance about cybersecurity. In fact, your employees are probably compromising your data right now and aren't even aware of it.

In case you haven't read the reports, a statement from one of the many companies recently forced to close its doors following a cyber-attack involving one of their own employees brings the point home:

"Code Spaces will not be able to operate beyond this point. The cost of resolving this issue and the expected cost of refunding customers who have been left without the service they paid for will put Code Spaces in an irreversible position both financially and in terms of ongoing credibility."

Root cause of the disaster? Very likely a phishing attack that one of their own team members unwittingly played a key role in.

If you want even a ghost of a chance that your data remains safe and secure, you MUST be aware of the five ways your employees are probably putting your company at risk right now:

Risky Passcode Practices

A good rule of thumb is if you can recall a password, it's probably not safe. Require the use of a random password generator to keep weak passcodes from being the weak link in your data's defenses. Invest in a company-wide password protection system. Wherever possible, using two -factor authentication for logins to critical sites is an excellent practice.

Working Outside A Secured Network

It's great that your team loves to collaborate. Just make sure it's done in a secure network. E-mail-sharing and file-sharing over a

Continued pg.2

non-secured network can lead to leaks. Train your team to share sensitive messages and files only within a secure company network. Even better, invest in encryption and collaboration tools that keep your data extra-safe while in transit. After all, great teams need to collaborate. Just make sure it's getting done without putting your data at risk.

"Safeguard all data coming into or going out from your company."

E-mail Naïveté
Most people are aware by now that clicking on unknown links in an e-mail can lead to trouble. Yet clever hackers are sending ever more appealing e-mails that trick the unwary into clicking. Insist that no attachments from unknown sources are to be opened. Require that users on your network look up unknown links before blindly clicking on them.

Unattended Devices
Walking away from an open laptop in a coffee shop is a recipe for disaster. Yet even at the office, stepping away from a workstation can expose sensitive data to snoops. Insist that wherever your team works, they maintain complete visual control over any screen showing confidential company data.

Malicious Acts
You may find it hard to believe, but employees leaking critical data on purpose happens all the time. It may be for a personal venture – or a personal vendetta against your company. Regardless of the cause, it's always a risk that you may not necessarily see coming. Safeguard all data coming into or going out from your company. Always change access codes whenever someone leaves your company – willingly or unwillingly.

Need an ally to help protect your data from employee sabotage – accidental or otherwise? Don't fight this battle alone – neoRhino can help!

Protecting company data in today's fluid and fast-changing business environment is tough work. If you don't have a robust protection plan in place, your critical data IS at risk. Our **Data Security Review** helps you and your team fend off attacks on company data. It also shows you the weak spots so you can seal them off from attack.

Call us today at **281-779-4850** or e-mail us at **info@neorhino.com** for more information. neoRhino IT Solutions would like to provide this vital, risk-reducing service to you because safeguarding your data is at the forefront of what we do best every day.

Windows Tip of the Month by Ed Bott

Create a System Image Backup

The surest way to recover from a data disaster, such as a system drive failure, is to restore that drive from an image-based backup. You'll need an external hard disk--at least as large as the amount of space in use on the system drive and ideally the same size as your system drive.

The capability to back up and restore a system image is in the Windows 7 Backup And Restore program. That same program is also in Windows 8, 8.1, and 10, although it's somewhat hidden. (In Windows 10, you can find it by typing backup in the search box.)

To start the program, press Windows key + R to open the Run box, type sdclt, and press Enter. Click Create A System Image from the column on the left, choose your external hard disk as the location where you want to save the backup, and click Next. On the following page, all partitions on the system drive should be selected. Just click Next and then click Start Backup.

Services We Offer:

- Network Cabling
- On-Site Help Desk Support
- On-Site Network Engineering including:
  - Cisco
  - Microsoft
  - Hyper-V & VmWare
- Disaster Recovery & Business Continuity
- Remote Managed Services
- Architecting and Implementing Enterprise Level Hardware Solutions

Give us a call today at 281-779-4850 to discuss your needs.

Free Report: The Business Owner's Guide to IT Support and Fees

You will learn:

- The 3 most common ways IT services companies charge for their services, and the pros and cons of each approach.
- A common billing model that puts ALL THE RISK on you, the customer, when buying IT services; you'll learn what it is and why you need to avoid agreeing to it.
- Exclusions, hidden fees and other "gotcha" clauses IT companies put in their contracts that you DON'T want to agree to.
- How to make sure you know exactly what you're getting to avoid disappointment, frustration and added costs later on that you didn't anticipate.

Claim Your FREE Copy Today by contacting us or by visiting our website at www.neorhino.com/newsletter.

3 Ways to Manage Someone You Hate

By Mike Michalowicz

Hate your co-worker or employee? Congratulations! You have completed the first step in making things work. Acknowledging you have a problem, after all, is the first step.

Ironically, teams where everyone likes each other are typically weak teams. People (that includes you) have a tendency to like people who are like them. We revel in similarities. Yet a team of copycats will have tunnel vision and won't have complementary skills. Great teams don't *like* each other nearly as much as they *respect* each other. There is greatness in differences.

Abraham Lincoln was famous for building a political cabinet of personal enemies. In a country that was polarized by a horrific civil war, Lincoln's genius was to assemble a cabinet of people who were his sworn enemies. Members of his cabinet may not have liked him (or vice versa), but it served what the country (client) needed.

Your company has a mix of clients with different needs and demands of their own. Your company has a mix of things to do, which requires special talents. Your company needs diversity, but along with that may come personal conflict (just ask Abe). Here is how you manage the people you hate:

1. Stop Trying To Like Them – A big fallacy of managers is to believe they need to like the person they are managing. That is not the case at all. The manager just needs to respect what the employee does. And when I say "respect," I mean to see genuine value in a talent or ability of that employee. Stop trying to find things to like about the employee you hate – find something to respect.

2. Find The Bigger Enemy – My consulting group was engaged to help grow a business run by two sisters. The problem was finger-pointing. Each sister blamed her struggles on the other, and they hated each other. That was until they found out their father was diagnosed with cancer. Immediately they had an enemy (the cancer) much greater than their hatred for each other. Instantly they started to work together amazingly well. Seek to find a common enemy (perhaps a competitor) that you and the employee you hate can target together. A common enemy makes the best of friends.

3. Distance Makes The Heart Grow Fonder – Short, temporary bursts of disgust trump a continual stream. If you just can't get over the fact that you can't stand the employee you manage, put distance between you and the employee. Put them in a different part of the office, or in a different office altogether. Of course, you can fire them too…but we are working under the understanding that you have an employee who is great at their work – you just can't stand them.

If Abraham Lincoln was able to manage a cabinet full of enemies and put a struggling country back onto the track to greatness, I think you just might be able to manage those employees you don't like (but respect) and put your company back onto the path to success.

MIKE MICHALOWICZ (pronounced mi-KAL-o-wits) started his first business at the age of 24. 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*" and his newest book, *The Pumpkin Plan*.

Become an influencer in your industry with these 3 blog hacks.

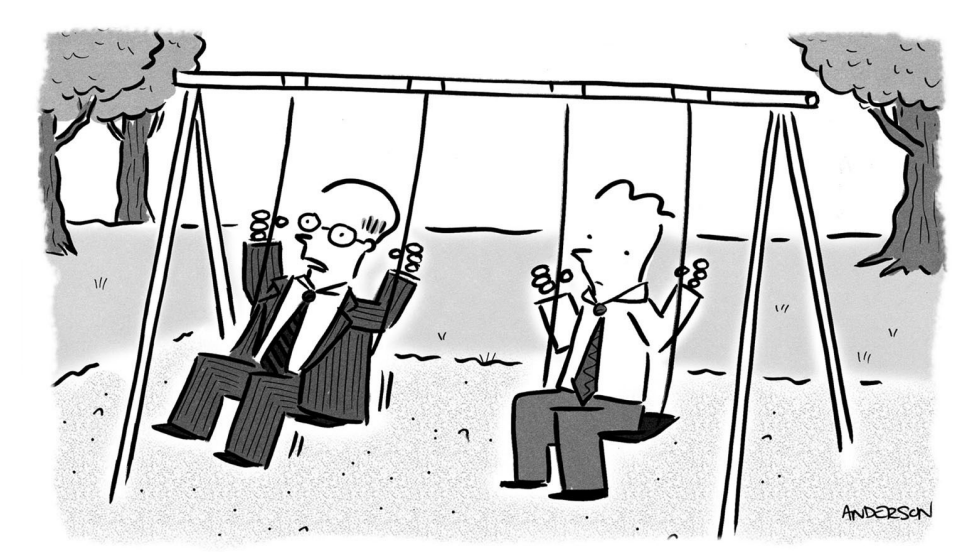
Building a "tribe" on social media with your blog can help drive sales for your business. Here are three ways to build it fast, and make it last. *1) Content is king.* Leave out the blurry iPhone pics. Mediocre content is no way to build an audience. Make it "good to great," or leave it out. *2) Originality wins.* Forget what you learned in school… Break rules and get creative to stand out. Top bloggers all share personal, unique and original content. That's what your audience cares about most – your unique voice and perspective. *3) Collaboration is key.* Connect with other bloggers to exchange audiences and/or content. This one tactic alone can help you reach millions of new readers.
-*Entrepreneur.com*

The average cost of a data breach keeps rising.

According to a recent study by IBM, excluding mega-thefts like the Sony hack, the overall average total cost per incident is around $4 million. Yet costs vary by industry. A health-care firm that deals with highly regulated and intimately detailed patient records may see a cost per stolen record at $355. At the other end of the spectrum, cost per stolen record in the public sector is closer to $80. Having an incident response team on hand cuts cost per stolen record by $16 a pop. Use of encryption saved an average of $13, employee training $9 and appointing a chief information officer $7. The report shows that how and when you respond to a cyber-attack can reduce the cost of recovery.
-*Fortune*

The Body Cardio scale by Withings introduces a whole new health metric.

It measures "Pulse Wave Velocity" (PWV), giving you insight into your heart health. Besides PWV, it also displays weight and body mass index (BMI). It even displays a weather report so you can check your weight before getting dressed. Other metrics include body fat, water percentage, muscle mass and bone mass. The Health Mate app it pairs with offers health and weight tips, trends and encouragement. At 0.7 inches "thin," it features a tempered glass top and an aluminum back. While Withings's claims about PWV aren't regulated by the FDA, Paris cardiologist Dr. Pierre Boutouyrie says, "If we could have just one measurement for cardiovascular health, it would be Pulse Wave Velocity."
-*DigitalTrends.com*



"I'm not much of a golfer."

The 8-hour workday is as outdated as the manual typewriter.

If you want to get a whole lot more done in your day, it's time to rethink how you structure it. Working eight hours per day started in the industrial revolution as a way to limit the number of hours workers had to endure on the factory floor. Yet a recent study by the Draugiem Group found that the ideal work-to-break ratio was 52 minutes of work with a 17-minute break. Folks who do that turn out to have a unique level of focus in their work. They're able to crush their competition because that's how the brain naturally functions. Structuring your day in this way can help you beat frustrating distractions and boost your productivity.
-*Forbes*

Here are 3 must-have apps for the type-A personality in your life. Could that be you?

Hate2Wait is a godsend for folks who can't stand to queue up. It estimates restaurant wait times and lets you reserve a table instantly. Spam is the bane of goal-driven people. It distracts and takes time to clean up. Put *Unroll.me* on your iPhone and link it to your e-mail accounts. It then lists every newsletter and promotion you're getting, and lets you lump them all into one e-mail address, keeping your in-box clear and clutter-free. Type A's love tracking their finances. *Mint* tracks all your money in one place, making budgeting and expense tracking a breeze. Just the thing for the type A in your life.
-*PCmag.com*