

August already, half way through summer. While we enjoy beach days, BBQs, vacation and relaxing in the dog days of summer, sadly Cybercriminals aren't letting up.

How bad is it getting? President Obama last month announced the US government was incorporating better ways to inform the public on what to do ONCE they have been attacked. Re-read that line. The President didn't say "If", he specifically said "Once". Getting hacked is the reality in this digital day and age.

Get Cyber Safe is the Canadian Government's response, providing information to help Canadians protect themselves. Check out the free tips and tools at:  
<http://www.getcybersafe.gc.ca/>

What measures do you have in place to protect your clients, your company and your ability to survive such an attack? **Contact us for a security assessment 506-383-2895**



**Happy New Brunswick Day!!**

## August 2016



This monthly publication provided courtesy of Scott Beck, President of BeckTek.

"As a business owner, I know 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 once and for all!"



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

**T**he 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

Passwords should be complicated and use at minimum one CAPITOL letter, a small case letter, a number and a symbol. Passwords should be changed on a regular basis and you shouldn't use the same password for all your devices and website accounts.

### 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 non-secured network can lead to leaks. Train your team to share

*Continued pg.2*

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.

### 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. And 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. And you may not see it coming. Safeguard all data coming into or going out from your company. And always change access codes whenever someone leaves your employ – willingly or unwillingly.

**Need an ally to help protect your data from employee sabotage – accidental or otherwise? Don't**

**fight this battle alone – our Data Security Review 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 (506) 799-2100 or e-mail [wendy@becktek.ca](mailto:wendy@becktek.ca) to book your **Data Security Review** right away. It's valued at \$497, but we'd like to provide this vital, risk-reducing service to you at no cost when you schedule it before August 31.

Safe data practices by your employees are absolutely critical to your company's success and survival. Contact us today for your free **Data Security Review**

*“Safeguard all data coming into or going out from your company.”*

## Free Report Download: The Business Owner's Guide To IT Support Services 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 at <http://www.becktek.ca/buyersguide/>**

## Shiny New Gadget Of The Month



## A Great Night's Sleep In The Palm Of Your Hand

The techno-geeks over at Hello Inc. have just released Sense, a device that helps you wake up feeling great. A tad smaller than a baseball, this little sphere sits on your nightstand next to your bed and monitors conditions in your room while you sleep. Things like temperature, humidity, light and sound in your bedroom are tracked, along with your body's slightest movements as you sleep. It pairs with your smartphone so you can see patterns and change conditions in your room to get the best night's sleep possible. Sense can play any number of soothing sounds to help you drift off to sleep. Then, when it's time to rise and shine, it gently wakes you up at the best time in your sleep cycle. It's priced at \$129, and you can find it at [hello.is](http://hello.is) and other online retailers.

## 3 Ways to Manage Someone You Hate

Hate your coworker 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, 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 Proventus 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/](http://www.mikemichalowicz.com/).

### 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 8-hour workday is as outdated as the 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

### Wise Words

*Failure is not falling down but refusing to get back up - Chinese Proverb*

© MARK ANDERSON, WWW.ANDERZTOONS.COM



"I'm not much of a golfer."

### What We Are Reading



Most people celebrate TGIF, excited to get away from the office and co-workers for a couple of days. What if you could get just as excited about getting back into the office?

*Thank God It's Monday* presents a unique approach to change the work environment from a “why we can’t” type negative atmosphere into a “how we can” workplace with a spirit of “bring it”.

I had my doubts thinking the book was just “touchy feely mumbo jumbo” but quickly realized Roxanne’s concepts are easy to understand and even easier to implement. She presents the roadmap to make TGIM possible !!

Banish negativity in your office, and start truly enjoying your work and co-workers—to love your job. It doesn’t matter if you’re an employee or the owner—the concepts can work for everyone.

Be the first to email the title of the book to me [scott@becktek.ca](mailto:scott@becktek.ca) and I will send you a free copy.