TECHNOLOGY TIMES

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

Did you get it?

BlackBox Connections has a **FREE Executive Brief!**

"The 7 Most Critical IT Security Protections Every Business Must Have In Place Now To Protect Themselves From Cybercrime, Data Breaches And Hacker Attacks"

Request your e-copy today!

Contact us at 403-451-0132
Or email
ask@blackboxconnections.com

January 2018

This monthly publication provided courtesy of:

Jason Mirosh
President
BlackBox
Connections

Our Mission: Tech to propel people to better connect, drive collaboration and share ideas in the business ecosystem.

Missing Just One Of These Could Instantly Open Up Your Computer Network To A Cyber Attack

Welcome to the brave new world of cyber-warfare.

Gone are the days when software patches were just for nifty little feature add-ons or updates.

Today, a software update notice could mean your whole computer network is suddenly at risk. Dangers include data theft, crippling malware attacks and mischief you may not discover for months, or even years…

As with graffiti on your garage door, if you don't pay attention and clamp down on bad behavior, your problems have likely just begun…

And, like those who hire a professional security firm to keep thieves out of the warehouse, thousands of CEOs and business owners are now waking up to the fact that it's absolutely imperative to hire a pro when it comes to securing your data network.

Here's why you need a professional handling this for you:

#1: Speed is of the essence.
"If you didn't update to version 7.32 within seven hours, you should assume you've been hacked." That's what software maker Drupal told millions of its customers around the world last year. It's just one example of what can happen if you don't respond with lightning speed.

Once a security breach has been identified, hackers rush in. On "Day Zero," cyber-crooks around the world go after at-risk targets. You've got to be quick to patch the gap, or else you risk a system compromise.

Unless you have the time, knowledge, experience and tool set to respond instantly, you are far better off leaving this to a professional IT firm you can trust.

#2: It's not just the big boys they're after.
Sure, the top news stories are about the attacks on companies like Target, Home Depot and Sony…

Yet your business is just as vulnerable, if not more so. Chances are, you simply do not have the resources that giant corporations have to manage a data disaster. The statistics bearing this out are shocking: more than 60% of small businesses close their doors following a serious data breach.

The threat is not confined to giant corporations. Small and medium businesses are being attacked every day, and, unfortunately, your business is no exception.

> “Chances are, you simply do not have the resources that giant corporations have to manage a data disaster.“

#3: Dealing with data breaches requires specialized knowledge, skill and experience.
Here are just a few of the things a competent data guardian must be able to do to effectively protect your systems:

Review documentation and monitor forums. Sometimes your software vendor doesn’t tell the whole story. It’s critical to check online forums and other communities to see if anyone else is having issues with the new patch before jumping in with both feet.

Know when to apply a patch immediately and when to wait. Typically, somewhere around 95% of patches work hassle-free. The trick is to spot the 5% that don’t — *before* installing them. This requires identifying unique patching requirements, and applying exceptions accordingly. For instance:

Does the patch deal only with a security issue?
Or does it just add new features or fix non-security-related bugs? Obviously, security issues get top priority.

Is the system currently having issues?
If not, and if the patch doesn’t address a security issue your system is vulnerable to, it may be better to heed the old adage “If it ain’t broke, don’t fix it.”

What security gaps does it address?
How severe is the threat to your particular network? If, for example, the only way a virus can enter your system is through an e-mail attachment and this functionality has been disabled for all users, perhaps the threat needn’t be a great concern.

Keep options open in case of complications.
Once a patch has been applied, if things aren’t working, it’s critical to restore the data network to pre-patch functionality, with little if any downtime. That means having good backups in place along with a tested and proven recovery process.
Does just thinking about data security give you a headache? We strongly advise that you let us handle this critical part of your business for you.

Call (403) 451-0132 and schedule our Security Update Audit today. You’ll discover how easy it is to rest assured that your network is secure 24/7.

IT Security Tip Use STRONG Passwords!

Thanks to powerful brute-force-attack software readily available online, hackers can try tens of millions of possible password combinations per second. For example, hacking software can guess a five-character password in under three hours. If you only use lowercase letters, it’s 11.9 seconds.

You KNOW you need to have a better password than “password” or “letmein” if you have any hope of keeping hackers out of your PC; but what does a “strong” password mean? A good password should be at least eight characters long (or longer!) and have a combination of uppercase and lowercase letters, numbers and symbols that are hard to guess.

Don’t use dictionary words with proper capitalization because they’re easy to guess (like **Password123X**). Even though it meets the requirements we just discussed, it’s easily hacked; remember, hackers have sophisticated password-hacking software that will run **24/7/365.**

Network Flaws That Lead to Data Loss ...

Data loss is one of the worst things that can happen to a business. The information you store on your servers is so important to your future success that it is critical you proactively take the steps to avoid common network flaws that lead to data loss. There are so many threats out there to your data that it's hard to keep up. It is important that you have a strong IT plan, and experts to implement that plan and provide you with ongoing advice.

The most common network flaws that you will want to avoid:

Weak Backup Systems – your backup is your most important line of defense against data loss. You must have onsite and offsite backups using strong backup software to protect your business in the event of any kind of issue, whether it's hardware failure, software corruption, human error, fire, flood or other disaster.

Poor Network Firewall – a firewall is supposed to block dangerous traffic from coming onto your network and secure you against mistakes by individual users. Many firewalls are poorly configured and maintained, leading them to be the IT equivalent of Swiss cheese security. This vulnerability can lead to data theft and loss.

Multi-layer Anti-Virus Protection – many viruses, especially new ransomware, can wreak havoc on your data and do permanent damage. Many businesses don't have proper multi-layer anti-virus security through firewall, desktop anti-virus and anti-spam measures.

Lack of User Education – the biggest security risk on any network is human error or negligence. Everyone should know better by now! But that doesn't mean you shouldn't regularly train your staff.

Poor Network Management and Maintenance – your IT systems are like your car, in order for them to keep running effectively and securely, they need to be properly managed and maintained. Data loss comes often from neglect of security updates Get an expert (us) who can help you effectively!

Top Time Saving Tech Tips

Time is Money and Money is time - Try these awesome working tips to save you time!

Scrolling up and down on a website Instead of using the mouse, press the space bar to scroll one page down, and hold the shift key + space bar to scroll up a page.

Filling in online forms - When you are required to select a City from a drop-down list, type in the first letter of the City and keep pressing the first letter to scroll through all the options that begin with that particular letter.

Changing text size on a website - To increase the size of the text on the screen, hold down the "Ctrl" key and hit the "+" key simultaneously until you reach the desired text size. To decrease text size, hold down the "Ctrl" key and hit the "-" key simultaneously.

Selecting text - Rather than using the mouse to select, delete, or move text in a document, use these time-saving tips instead:

- Highlight a word: Double-click the word.
- Highlighting a paragraph: Triple-click to select all the text in a given paragraph.
- Deleting words: Don't delete word by word. Highlight and type over the entire text.

Connect with us and let's donate to
"**Alberta's Promise Partners**" for children who
could use something that will educate
them for the future!
BlackBox Connections will
come pick up your forgotten,
unused, dusty computers and
make them like new for **FREE.**
Contact us today **(403) 451-0132**

PROUD **PARTNER** OF
ALBERTA'S PROMISE
www.albertaspromise.org

6 Quick Tips To *Finally* Organize Your Out-Of-Control Inbox

Much like laundry and bills, no matter how much you try to keep up, e-mails just keep piling up in your inbox. E-mail is a critical part of your day-to-day work, so how do you keep it from becoming a distraction while balancing the things you really need to address? Here are 6 tips…

1. **Zero your inbox**. Do you remember the last time your inbox was empty? Probably never; that's because it costs nothing to keep an e-mail and therefore you don't delete items "just in case" you need them at some point. This really causes messages to pile up FAST. Truth be told, you really DON'T need all those e-mails. Make it a goal to "zero" your inbox every week, particularly on a Friday before you leave for home. If you can't "zero" it, at least get the number down to fewer than a dozen critical messages you absolutely need to work on within the next 2-3 days.

2. **Use folders sparingly.** Only set up key, strategic folders or you'll end up with dozens of folders filled with messages in addition to a massive number of messages in your inbox. You might keep one labeled as "storage" for any non-urgent messages that may need to be referenced at a later date. This keeps your inbox free of clutter and helps you more easily find something in an old message when it is needed.

3. **Delete first, read the surviving messages later.** Many of the e-mails you get probably aren't even worth reading. Start your day by immediately deleting these emails before you even start to open and read the important ones.

4. **Take action immediately.** Probably the most helpful way to keep your inbox uncluttered is to take action right away on all messages instead of reading them and then going back to them later when you have time to process the message properly. By taking action right away you avoid wasting time re-reading messages. If it does require a follow up that you don't have time for, file the message and mark a reminder to follow up. Otherwise forward it, delete it or file it into a folder

5. **Slow your roll.** Your e-mail can be a constant distraction through your workday, IF you let it! Take control and set aside "e-mail free" time periods throughout the day so you can truly concentrate on projects without interruption. The world won't stop if you don't check your email every few minutes, I promise.

6. **Install a GOOD spam filter.** The vast majority of messages are unwanted spam, some of which contain viruses. But not all spam filters are created equal!