Bits & Bytes

Insider Tips On How To Use Technology To Make Your Business Run Faster, Easier, And More Profitably

5 Steps To Protect Your Business From Cyber Crime

> *"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 forever."*
>
> **Joe Stoll, President**
> Technical Action Group (TAG)
> JStoll@TechnicalActionGroup.com

Inside this issue:

A Seattle company was recently broken into and a stash of old laptops were stolen. Just a typical everyday crime by typical everyday thieves. These laptops weren't even being used by anyone in the company. The crime turned out to be anything but ordinary when those same thieves (cyber-criminals) used data from the laptops to obtain information used to siphon money out of the company via fraudulent payroll transactions. On top of stealing money, they also managed to steal employee identities.

Another small company was hacked by another "company" sharing the same high-rise office building with them. Management only became aware of the theft once they started seeing unusual financial transactions in their bank accounts. Even then, they didn't know if there was internal embezzlement or external cybertheft. It turned out to be cyber-theft. The thief in this case drove a Mercedes and wore a Rolex watch… and looked like anyone else walking in and out of their building. Welcome to the age of cybercrime.

You Are Their Favorite Target

One of the biggest issues facing small businesses in the fight against cybercrime is the lack of a cyber security plan. While 83% lack a formal plan, over 69% lack even an informal one. Only ½ of small business owners believe that cybercrime will never affect them. In fact, small businesses are cybercriminals favorite target! Why? They're not prepared and they make it easier on them.

The result? Cyber-attacks cause SMB's an average of $188,242 each incident and nearly 2/3'rds of the businesses affected are out of business within 6 months. (2011 Symantec/NCSA Study) A separate study by Verizon showed that over 80% of small business cybercrime victims were due to insufficient network security (wireless and password issues ranked highest). With insecure networks and no formal plan to combat them, we make it easy for them.   While these are US stats, Canada is not immune.

How They Attack

The #1 money generating technique these "bad guys" use is to infect your systems with malware so that whenever you (or your employees) visit a website and enter a password (Facebook, bank, payroll, etc.) the malware programs harvest that data and send it off

Shiny Gadget Of The Month:

The 30-Day Lantern

It's summer time and that means more outdoor activities. This 30-Day Lantern is the perfect companion for your cookouts and camping trips. Not to mention, it's a handy gadget to keep in your vehicle or garage for those emergency situations when power is down.

This lantern provides up to 30 days of reliable light on one set of batteries. The lantern generates up to 300 lumens of bright, white light that can be seen from up to 75 1/2' away. Made from impact-resistant ABS with rubberized encasements, the lantern is shock- and water-resistant. The device has a green LED that flashes when the device is off for easy location in blackouts and a built-in hook allows the lantern to be hung upside down. With three light output levels and a flashing mode (provides 32 hours of light on high).

Get your lantern at www.hammacher.com

---

to the bad guys to do their evil stuff.

They can get to you through physical office break-ins, "wardriving" (compromising defenseless wireless networks) or email phishing scams and harmful websites. Cyber-criminals are relentless in their efforts and no one is immune to their tricks.

5 Steps To Protect Your Business

Get Educated. Find out the risks and educate your staff

Do A Threat Assessment. Examine your firewall, anti-virus protection, and anything connected to your network. What data is sensitive or subject to data breach laws?

Create A Cyber Security Action Plan. Your plan should include both education and a "fire drill".

Monitor Consistently. Security is never a one-time activity. Monitoring 24/7 is critical.

Re-Assess Regularly. New threats emerge all the time and are always changing.

You can only win by staying ahead!

---

3 Solutions To Minimize The Risk Of A Server Crash

Servers are one of most powerful pieces of equipment in the office, but that does not mean they are the toughest. The hard drives in servers are made up of ridiculously fast moving parts. One day, these small parts will fail and end the server's life with a sudden crash. Here are a few steps you can take to prepare for server doomsday.

Because crashing is an eventuality, manufacturers will recommend that you cycle out your old server for a new one every 3 years. For companies on a tight budget, this recommendation may fall on deaf ears, but there is truth to this advice that goes beyond profits. The reason for this recommendation is because servers are designed with a 99.5% uptime. These moments of downtime are more likely to take place towards the end of the server's lifespan, which will typically be beyond the 3 year mark. With a new server, you may see little-to-no downtime in years 1-through-3, but after that, you may experience more downtime during your fourth year than in years 1-through-3 combined.

Backup with a BDR

The prospect of your server crashing and losing your data is a real risk. The first thing you will want to do is make sure the data on your server is backed up. We recommend using a Backup and Disaster Recovery (BDR) solution. A BDR will backup all of your server's data offsite; this way, if there is ever a disaster, such a hard drive crash or an even worse disaster like fire, theft or flood, your data will be safe and can quickly be retrieved using a replacement server.

Virtualize Your Servers

If your business has been maintaining an IT network for a few years, then you may have accumulated multiple servers. You may even be using a few server units that are older than three years old--these older units may be the likely culprits behind several of your network's problems. The reason you may have extra server units is because, in the past, the purchase of a new application used to require the purchase of a new server. These dedicated servers hosting only one app might have only been utilized by 20-to-30%, and newer server units are more powerful than ever.

With server virtualization, we can take your most powerful servers and consolidate the applications of older servers into newer units that are underutilized. With a server virtualization makeover, you will be able to consolidate 3-to-10 applications into one server. This will allow you to junk the older servers that have been causing you problems and minimize the risk of a server crash.

Virtualize Wisely

Server virtualization is a great way to minimize the risks of a server crash, but it will not completely eliminate the risks. The hard drives on your servers are still at risk of crashing due to tiny parts moving at thousands of revolutions per minute. Another step you can take to minimize the risk of a crash is to be smart about virtualizing your applications. You will do this by moving your most mission-critical applications to your newest and best servers. These are the applications that you use every day and are accessed by everyone in your company. In contrast, you likely have additional not-as-important applications on your network. Your medium-grade server units would be a good home for these apps. This way, if the medium-grade server goes down, then all of your mission critical applications will still be online.

TAG can provide you with a BDR solution, as well as consolidate your server units with server virtualization. Both of these procedures will minimize the risks associated with a hard drive crash. These are just few of the ways TAG can protect your business from downtime. With our managed IT services, we can remotely take care of computer maintenance and keep all of your PCs running smoothly. Call Joe Stoll at 416-489-6312 x 204 or JStoll@TechnicalActionGroup.com to learn more.

4 Tips Not To Be "That Guy"

The cool thing about using mobile devices equipped with tools that will allow you to remotely access your company's files from anywhere, is that you now have the freedom to work from literally anywhere. Just be careful not to abuse this freedom. Here are 4 tips to help you work on the go without annoying everybody around you.

If you are venturing to a public place, like a park, coffee shop, or airport, to work on a project on your mobile device, it's important that you understand how different the outside world is from your office. A public space has different behavioral expectations, commonly referred to as etiquette, which can be much different than your private office. If you break these public etiquettes, then you are no better than that one annoying guy who makes a scene in public; in fact, you are that guy!

Isolate Yourself When Taking Phone Calls

Taking phone calls is a big part of working remotely. If you are working in a public setting and find yourself surrounded by people, you may think it's acceptable to whip out your cell phone to get work done, but it's not. You may think that talking on your phone in public is no different than two people carrying on a conversation, but it's very different. Two people having a face-to-face conversation in public can adjust their volumes to match what's appropriate for their surroundings. A person on the phone may need to talk louder to be heard better, and therefore may not have the option to talk quieter. If you must talk on the phone in public, it's good etiquette to step outside and remove yourself from the group.

Watch Your Temper

In your office, you rule the roost. You can explode at employees and people know to tiptoe around you when you are having a bad day. Outside of your kingdom, things work differently. In the eyes of the public, nobody cares how big your business is, you are just another schmo; and if you are taking up a whole table with all of your gadgets, then the public is already viewing you with suspicion, just waiting for you to do something stupid. Don't confirm their suspicion by having a temper tantrum for all to see. Emotions are weird, and showing your emotions to a public that's not expecting to see them, especially anger, will make everyone around you feel uncomfortable.

10 Ideas You Need If You Want To Succeed

1. Do what you need to do now so you will eventually get to do what you want to do later.

2. Discipline is the ability to get things done regardless of how you feel about doing them.

3. Passion only pays off when channeled into productive effort.

4. Others may believe in you, help you and support you, but ultimately nobody will do it for you. You are responsible for your own life.

5. If you don't do your job any differently than anybody else who does it, you won't get paid more than anybody else.

6. More often than not, you succeed in spite of not because of your circumstances.

7. If you think a little better and work a little harder you will always accomplish more than others.

8. If you can't control it, get over it.

9. If you don't appreciate where you are at, you won't appreciate where you are going.

10. Get clear on what really matters to you and then get busy pursuing it.

If you want more insights into how to turn the ordinary into the extraordinary, go to www.marksanborn.com

Sometimes you'll get a message from a new contact that isn't included in your Outlook Contacts yet. It's easy to add the sender's info directly from the message they send.

When you get a message from a new contact, simply right-click on their name in the Reading pane, or in the e-mail and select "**Add to Outlook Contacts.**"

A Contact window will pop open with their name and email address filled in. From here you can add any additional information you have for them that you need and click Save. You can enter in their second email address, work or home address, phone number, IM handle, birthday, and any additional notes you need.

You can do the same thing in Outlook 2007, but the process in Outlook 2010 and 2013 and 365 is a much cleaner and fluid experience.

Don't Forget Your Headphones

Whether you are having a video conference from your laptop, need to watch a training video, or even listening to your favorite tunes, it's always a good idea to use your headphones. Public places are noisy enough on their own; nobody wants the noise from computer speakers added to the chaos.

Keep the Size and Loudness of Meetings Appropriate to Your Surroundings

Meetings of any size can be difficult to control and can easily become too loud. One of the worst things you can do is show up to a small public place with a large group and essentially "take it over." A situation like this may make it even more difficult to control your people because they may feel emboldened to be louder, especially if they feel like they have a majority share in the public venue. Even with a remote meeting on your PC, you will want to be aware of your surroundings and volume level so it won't distract everyone else.

3 Ways We Relieve Your Pain Points!

What are your biggest pain points? Some pain points are obvious, like the issue keeping you up at night. Other pain points are smaller; you may not worry about them as much, but they still affect your bottom line. Here are 3 ways we can help find solutions for some of your company's pain points.

We Learn About the Obvious Pain Points

When we talk with you about your business, we take the time to listen. This may seem like an obvious business strategy, but you would be surprised by how many businesses won't listen to their customers. You may have experienced this yourself whenever you called up a large company with a problem, only to be transferred through a maze of different departments.

What makes TAG's IT different is that we are an IT solutions company. This means that we see it as our job to learn everything we can about your problem, and then find you the best solution possible. Our solutions approach means that you are not just another customer with a random account number, you are our client and we will take the extra time to learn about the pain points weighing most heavily on your mind.

We Notice Pain Points that are Hidden

One advantage that comes from taking time to listen is that we are able to discover pain points that you may have missed. We are able to uncover these hidden pain points because of our years of experience finding IT solutions for a variety of businesses. Looking for these hidden pain points is important because sometimes, the obvious problem may stem from an issue that's not-so-obvious to the untrained eye. Taking care of these root issues is the best way to take care of a pain point. It's the difference between popping a pain pill to relieve a symptom, or finding out what's causing the pain and then performing surgery to remedy the problem. A company that doesn't take the time to get to the bottom of the problem may only be able to offer their customers a cosmetic fix, which will then cause the pain point to resurface again, costing customers even more money.

We Identify with Pain Points that are Universal

There are many pain points that every business, including our own (we're not immune!) seem to always be experiencing. Let's take a look at budgeting as one example. Every business struggles with it; making it a universal pain point. Every business wishes they could spend less on IT, and more on things that are closer to their hearts, like salary or marketing. With TAG managing your IT infrastructure, your IT budgeting pain point is relieved because you can now categorize IT repair as an operating expense. If you subscribe to an all-inclusive plan, you can now budget for your IT expenses so your technology repair bill won't be a surprise that eats away at your profits. By determining pain points and having money freed in the capital column, our managed IT services will make your IT infrastructure profitable! This is the whole point of technology; to not have to worry about it, and instead, having your technology work for you. If your technically is a giant pain, give Joe Stoll a call at 416-489-6312 x 204 or e-mail JStoll@TechnicalActionGroup.com.