

The 8 Most Critical IT Security Protections Every Business Must Have In Place NOW To Protect Themselves From Cybercrime, Data Breaches And Hacker Attacks

Cybercrime is so widespread that it's not a matter of if your – large **OR** small – business will be attacked, it is a matter of **WHEN!** However, a few effective preventative measures **CAN PREPARE YOU** and minimize (or outright eliminate) any reputational damages, losses, litigation, embarrassment and costs.



Provided By: [Your IT Results Inc.](#)

Author: **Kelly Speers**

Suite 200, 1001 – 1 Street SE

Calgary, AB T2G 5G3

(403) 407 – 2443

www.youritresults.com

When You Fall Victim To A Cyber-Attack Through No-Fault Of Your Own, Will They Call You Stupid...Or Just Irresponsible?

It's EXTREMELY unfair, isn't it? Victims of all other crimes – burglary, robbery, mugging, carjacking, theft – get sympathy from others. They are called “victims,” and assistance and support comes flooding in.

But, if your business is the victim of a cybercrime attack and your client data is compromised there is NO sympathy. You will be instantly labelled as stupid or irresponsible. **You** will be **investigated** and **questioned about what YOU did to prevent this from happening** – and if the answer is not enough, you can be found liable, facing serious fines and lawsuits. You will be required by law to tell your clients that **YOU** exposed their private records, financial records and data to criminals. Your competition will have a heyday over this, and clients will leave in droves once they discover you've been compromised. Your bank will NOT come to your rescue, and unless you have a very specific type of insurance, **any financial losses may not be covered.**

Here's The Ugly Truth:

You already know that cybercrime is a very real threat to you – but it's very possible that you're underestimating the potential damage, **OR you are being ill-advised** and underserved by the employees and/or vendors you hired to protect your business from these threats.

ONE cyber-attack...one slipup from even a smart, tenured employee clicking on the wrong e-mail...can open the door to ABSOLUTE FINANCIAL DEVASTATION, and undo everything you've worked so hard to achieve. **Take the story of Michael Daugherty, former CEO of LabMD.**

His \$4 million Atlanta-based company tested blood, urine and tissue samples for urologists – a business that was required to comply with federal rules on data privacy as outlined in the Health Insurance Portability and Accountability Act, or HIPAA. He HAD an IT team in place that he **believed** was protecting them from a data breach – yet the manager of his billing department was able to download a file-sharing program to the

company's network to listen to music, and unknowingly left her documents folder (which contained over 9,000 patient files) open for sharing with other users of the peer-to-peer network. This allowed an unscrupulous IT service company to hack in and gain access to the file and use it against them for extortion. When Daugherty refused to pay them for their "services," the company reported him to the Federal Trade Commission, who then came knocking.

After filing some 5,000 pages of documents to Washington, he was told the information he had shared on the situation was "inadequate," and the FTC requested in-person testimony from the staff regarding the breach, and more details on what training manuals he had provided to his employees regarding cybersecurity, documentation on firewalls and penetration testing. **(QUESTION: ARE YOU ACTUALLY DOING ANY OF THIS NOW?)**

Long story short, his employees blamed HIM and left. Sales steeply declined as clients took their business elsewhere. His insurance providers refused to renew their policies. The emotional strain on him – not to mention the financial burden of having to pay attorneys – took its toll, and eventually he closed the doors to his business, jamming medical equipment into his garage where it remains today (image below).



“Not My Company...Not My People...” You Say?

Don't think you're in danger because you're “small” and not a big target like a J.P. Morgan or Home Depot? Or that you have “good” people and protections in place? Think again. Every single day in 2020, 350,000 NEW malware threats are being released, and more than HALF of the cyber-attacks occurring are aimed at small businesses; you just don't hear about it because it's kept quiet for fear of attracting bad PR, lawsuits and data-breach fines, and out of sheer embarrassment – but make no mistake: small businesses are being compromised daily, and the smug ignorance of “that won't happen to me” is an absolute surefire way to leave yourself wide open to these attacks.

In fact, the National Cyber Security Alliance reports that **one in five small businesses have been victims of cybercrime in the last year** – and that number is growing rapidly as more businesses utilize cloud computing and mobile devices and store more information online.

You can't turn on the TV or read a newspaper without learning about the latest online data breach, and government fines and regulatory agencies are growing in number and severity. **Because of all of this, it's critical that you have these seven security measures in place.**

But I Have A Great IT Guy I Trust...

Many business owners are shocked when they get compromised because they BELIEVED their IT company or guy had it “handled.” However, there is a virtual army of thousands of hackers and very sophisticated crime rings that work around the clock to overcome known protections – and you can't stop a brand-new threat that was invented yesterday with a security system that was designed six months to a year ago. It requires special expertise to stay on top of all of this, which is why many don't.

To that end, here's your quick 8-step checklist. If YOUR company isn't actually implementing ALL of these protocols – OR if you don't know if you are – WHY NOT? What hasn't your current IT company told you about all of this?

1. **The #1 Security Threat To ANY Business Is...You!** Like it or not, almost all security breaches in business are due to an employee clicking, downloading or

opening a file that's infected, either on a website or in an e-mail; once a hacker gains entry, they use that person's e-mail and/or access to infect all the other PCs on the network. Phishing e-mails (an e-mail cleverly designed to look like a legitimate e-mail from a website or vendor you trust) is still a very common occurrence – and spam filtering and antivirus cannot protect your network if an employee is clicking on and downloading the virus. That's why it's **CRITICAL** that you educate yourself and all of your employees on how to spot an infected e-mail or online scams. Cybercriminals are **EXTREMELY** clever and can dupe even sophisticated computer users. All it takes is one slipup, so constantly reminding and educating yourself and your employees is critical.

2. Implementing and enforce an **Acceptable Use Policy**. An **AUP** outlines how employees are permitted to use company-owned PCs, devices, software, Internet access and e-mail. We strongly recommend putting a policy in place that limits the websites employees can access with work devices and Internet connectivity. Further, you have to enforce your policy with content-filtering software and firewalls. We can easily set up permissions and rules that will regulate what websites your employees access and what they do online during company hours and with company-owned devices, giving certain users more “freedom” than others.

Having this type of policy is particularly important if your employees are using their own personal devices and home computers to access company e-mail and data. With so many applications in the cloud, an employee can access a critical app from any device with a browser, which exposes you considerably.

If an employee is logging in to critical company cloud apps through an infected or unprotected, unmonitored device, it can be a gateway for a hacker to enter **YOUR** network – which is why we do not recommend you allow employees to use their own personal devices to work remotely or from.

If that employee leaves, are you allowed to erase company data from their phone or personal laptop? If their phone is lost or stolen, are you permitted to remotely wipe the device – which would delete all of that employee's photos, videos, texts, etc. – to ensure **YOUR** clients' information isn't compromised?

Further, if the data in your organization is highly sensitive, such as patient records, credit card information, financial information, personally identifiable information (PII), and the like, you may not be legally permitted to allow employees to access it on devices that are not secured. That doesn't mean an employee might not

innocently “take work home.” If it’s a company-owned device, you need to detail what an employee can or cannot do with that device, including “rooting” or “jailbreaking” the device to circumvent security mechanisms you put in place.

3. **Require STRONG passwords and passcodes to lock mobile devices.**

Passwords should be at least 8 characters containing lowercase letters, uppercase letters, symbols, and at least one number. On a cell phone, requiring a passcode to be entered will go a long way toward preventing a stolen device from being compromised. Again, this can be **ENFORCED** by your network administrator so employees don’t get lazy and choose easy-to-guess passwords, putting your organization at risk. If you and your employees are not being forced to do a password reset every 30-60 days, **THEY ARE FAILING YOU**.

How long will it take to brute-force guess your password?

Length of password	Only numbers	Mix of lower and upper case letters	Mix of numbers, lower and upper case letters	Mix of numbers, lower and upper case letters, and symbols
8	Instantly	3 hours	10 days	57 days
9	4 seconds	4 days	153 days	12 years
10	40 seconds	169 days	1 year	928 years
11	6 minutes	16 years	106 years	71k years
12	1 hour	600 years	6k years	5m years
13	11 hours	21k years	108k years	423 years
14	4 days	778k years	25m years	5bn years

4. **Keep your network and all devices patched and up-to-date.** New vulnerabilities are frequently found in common software programs you are using, such as Adobe, Microsoft, and lines of business applications; therefore it’s critical you patch and update your systems and applications when patches become available. If you’re under a managed IT plan, this can all be automated for you so you don’t have to worry about an employee missing an important update.

5. **Have A Business-Class Image Backup BOTH On-Premise And In The Cloud.** This can foil the most aggressive (and new) ransomware attacks, where a hacker locks up your files and holds them ransom until you pay a fee. Hackers are waiting sometimes months before infecting, encrypting, and deleting your files. They wait until they have successfully corrupted your backups so that you can not restore from the backups you thought were safe. This is why you want to backup

to multiple locations as well as an offsite location. We encourage the rule of 3, your working copy, local backup, and offsite backup. If your files are backed up, you don't have to pay a crook to get them back.

A good backup will also protect you against an employee accidentally (or intentionally!) deleting or overwriting files, against natural disasters, fire, water damage, hardware failures and a host of other data-erasing disasters. Again, your backups should be **AUTOMATED, TESTED and MONITORED**; the worst time to test your backups is when you desperately need them to work!

6. **Don't allow employees to access company data with personal devices that aren't monitored and secured by YOUR IT department.** The use of personal and mobile devices in the workplace is exploding. Thanks to the convenience of cloud computing, you and your employees can gain access to pretty much any type of company data remotely; all it takes is knowing the username and password. Employees are now even asking if they can bring their devices to work (BYOD) and use their smartphone for just about everything.

But this trend has **DRASTICALLY** increased the complexity of keeping a network – and your company data – secure. In fact, your biggest danger with cloud computing is not that your cloud provider or hosting company will get HACKED (although that remains a possibility); the biggest threat is that one of your employees accesses a critical cloud application via a personal device that is infected, thereby giving a hacker access to your data and cloud applications.

So, if you ARE going to let employees use personal devices and home PCs, you need to make sure those devices are properly secured, monitored and maintained by a **CYBERSECURITY-FOCUSED** organization. Further, do not allow employees to download unauthorized software or files. One of the fastest ways cybercriminals access networks is by duping unsuspecting users into willfully downloading malicious software by embedding it within downloadable files, games or other “innocent” looking apps.

But here's the rub: most employees won't want you monitoring and policing their personal devices; nor will they like that you'll wipe their device of all files if it's lost or stolen. But that's exactly what you'll need to do to protect your company. We suggest that you allow employees to access work-related files, cloud applications and e-mail only via company-owned, secured, and monitored devices, and never

allow employees to access these items on personal devices or **PUBLIC WiFi**.

7. **A Business-Class Advanced UTM Firewall.** A firewall acts as the frontline defence against hackers blocking everything you haven't specifically allowed to enter or leave your computer network. But all firewalls need monitoring and maintenance, just like all devices on your network, or they are completely useless. This too should be done by your IT person or company as part of their regular, routine maintenance. HOWEVER, it's not uncommon for an IT guy to forget to turn on one or more of the intrusion detection and prevention features; often they are disabled to work on the firewall, but then never turned back on, making the device useless.
8. **Actively monitor the DARK WEB for when your company and user's credentials become for sale.** There are websites that sell your company's and your user's information, banking information, usernames and passwords to buyers who are interested in identity theft. Startlingly, the dark web is what you cannot Google and represents close to 99% of what is out on the internet.
(<https://curiosity.com/topics/the-deep-web-is-the-99-of-the-internet-you-cant-google-curiosity/>).

Are you willing to **RISK** not knowing when your employee's credentials have become for sale on the **DARK WEB** or when your companies usernames and passwords are being sold for \$2 per credential to HACKERS? You need to know when your information is being sold to hackers and have that information available to act on.

Are You **REALLY** Willing To Be **Complacent** About This?

Look, I know all of this appears to be a giant distraction and cost that interferes with REAL work. You and I both realize that implementing proper security protocols won't win you the "employer of the year" award or deliver an ROI – in fact, we HOPE by doing OUR job, it never has to deliver one.

BUT if you foolishly choose to turn a blind eye and be arrogant, complacent or careless, cybercriminals WILL take advantage of you. You WILL pay the ransom...NOT YOUR FAILING IT COMPANY that was SUPPOSED TO PROTECT YOU. This tsunami of pain will land directly on YOUR desk to deal with, everyone pointing the blame at YOU.

YOUR bank account. YOUR business. You will be faced with significant losses, costs and an emotional drain on you and your team as you deal with being HACKED.

Criminals do not care about the size of your organization. They cast a wide net hoping to catch something and often are surprised when they get the big fish. Knowing smaller organizations do not have the experience, team, or tools in place to protect themselves. In 2016 a single person running a dog rescue charity was hit with ransomware because she believed nobody would attack a small business or charity. She was wrong!

Ottawa

Dog charity pays hackers ransom to retrieve computer files



The dog rescue charity BARK is back in business after paying \$800 to rid its computer of ransomware

Steve Fischer · CBC News · Posted: Jun 08, 2016 5:00 AM ET | Last Updated: June 8, 2016



Mark Twain Once Said,

“Supposing Is Good, But KNOWING Is Better”

If you want to know for SURE that your current IT company (or IT person) is truly doing everything they can to secure your network and protect you from ransomware, bank fraud, stolen and lost data and all the other threats, problems and costs that come with a data breach, then you need to call us for a **FREE Security And Backup Audit**.

No cost or obligation, we'll send one of our security consultants and a senior, certified technician to your office to conduct a free **Security And Backup Audit** of your company's overall network health to review different data-loss and security loopholes, including small-print weasel clauses used by all third-party cloud vendors, giving them zero responsibility or liability for backing up and securing your data. We'll also look for common places where security and backup get overlooked, such as mobile devices, laptops, tablets and PCs. At the end of this free audit, you'll know:

- Is your network really and truly secured against the most devious cybercriminals? And if not, what do you need to do (at a minimum) to protect yourself now?
- Is your data backup TRULY backing up ALL the important files and data you would never want to lose – and (more importantly) how FAST could you get your IT systems back online if hit with ransomware? We'll reveal exactly how long it would take to restore your files (most people are shocked to learn it will take much longer than they anticipated).
- Are your employees freely using the Internet to access gambling sites and porn, to look for other jobs and waste time shopping, or to check personal e-mail and social media sites? You know some of this is going on right now, but do you know to what extent? Are they downloading illegal files (music and video) and exposing you, as happened with LabMD?
- Are you accidentally violating any data-privacy laws? New laws are being put in place frequently, and it's easy to violate one without even being aware; however, you'd still have to suffer the bad PR and fines if a breach happens and the investigation reveals YOU didn't take necessary precautions – and ignorance is not an acceptable excuse that will get you out of a lawsuit.
- Can your firewall and antivirus handle today and tomorrow's threat landscape? Is it configured properly and up-to-date? No security device is “set and forget.” It needs to be constantly monitored and updated – is yours? Is your IT company

giving you the assurances that it is?

- Are your employees storing confidential and important information on unprotected cloud apps like Dropbox that are OUTSIDE of your backup? Could they walk off the job with a list of all your clients and go work for a competitor?
- How much of your company's information is for sale on the DARK WEB?

I know it's natural to want to think, "We've got it covered." **Yet I can practically guarantee my team will find one or more ways your business is at serious risk for hacker attacks, data loss and extended downtime – I just see it all too often in the over 11 years of doing audits for businesses.**

Even if you have a trusted IT person or company who put your current network in place, it never hurts to get a third party to validate nothing was overlooked. I have no one to protect and no reason to conceal or gloss over anything we find. If you want the straight truth, I'll report it to you.

You Are Under No Obligation To Do Or Buy Anything

I also want to be very clear that there are no expectations on our part for you to do or buy anything when you take us up on our **Free Security And Backup Audit**. As a matter of fact, I will give you my personal guarantee that you won't have to deal with a pushy, arrogant salesperson because I don't appreciate heavy sales pressure any more than you do.

Whether or not we're a right fit for you remains to be seen. If we are, we'll welcome the opportunity. But if not, we're still more than happy to give this free service to you.

You've spent a lifetime working hard to get where you are. You earned every penny and every client. Why risk losing it all? Get the facts and be certain your business, your reputation and your data are protected. Call us at **(403) 407 - 2443** or you can e-mail me personally at kelly@youritresults.com.

Dedicated to serving you,

Kelly Speers

Web: www.youritresults.com

E-mail: kelly@youritresults.com

Here's What A Few Of Our Clients Have Said:

Trustworthy with the fastest response times



The team at Your IT Results Inc. helps us understand what we NEED to know to keep our systems and our clients information as secure as possible from hackers. They take the time to go through what we have and explain what needs to be replaced or added, keeping our budget in mind. They are great communicators, taking the time to talk to each of us without talking down to us. Very trustworthy people that we do not hesitate to refer.

Cindy G, Elbow Valley

Technical support in less than 60 seconds



In the Past, our technical support provider would have to try and fit us in, sometimes days later. Now, we call and are speaking to a technician from Your IT Results Inc. in less than 60 seconds. The worry is taken away from having to try and fix things ourselves or hope something doesn't go wrong outside of regular business hours with 24/7 coverage. Your team does not make us feel like we are idiots because we don't know as much about IT as they do. I wouldn't hesitate to refer Your IT Results Inc. and in fact I have already. ***Teresa J, Choice Memorial***

Our issues are as important to Your IT Results as they are to us



Trust is the foundation of any relationship, I put my trust in the team at Your IT Results Inc. knowing they are the IT experts so I don't have to be. I personally know two other business leaders who use Your IT Results Inc on of whom I referred to Your IT Results Inc directly. All of us would and do, without reservation and with confidence, refer their services to our own clients.

Lisa Demers, ABBA Books

Computer Security Is Priority #1



Cybersecurity for our company, as well as our client's data, is critical to us, and Your IT Results Inc. keeps us protected against the continually increasing threats. The help desk usually answers our calls live or within a minute, and they speak in easy to understand terms with NO GEEK SPEAK. Fast answer times and incredible service is why we recommend Your IT Results Inc!

Andrew H, Bercal Food Services Ltd.

Friendly, Professional, Knowledgeable and Prompt!



Our office is fast-paced and chaotic. We need to have IT support quickly, and Your IT Results Inc. provides answers right away. Our cybersecurity, computers, Microsoft 365, and suggestions on how to best use what we have and what is coming. The help desk team is knowledgeable and never speaks down to us while providing very prompt service. We 100% suggest going with Your IT Results Inc.

Sheri N, Sons of Electric

Quick response times even during the evenings and weekends



Your IT Results and their team operate with the highest level of integrity while providing customer service in an industry that it seems to be missing. They always seem to be available with quick answers to our questions or issues, this is critical to us because our volunteers often work evenings and weekends. They take the time to listen to our needs and work with in our budget to maximize the services they provide us. As a registered charity this is critical to us.

Jim M, Angels Anonymous.

"Customer service driven" Not just a tagline



I have highly recommend Your IT Results and their team to other business leaders, their customer service is unmatched. We have been clients for over 6 years and continue to rely on their expertise in cybersecurity, cloud services, and computer support. They are amazingly quick to answer emails or phone calls and work with us to find a solution that fits OUR needs. They put the needs of our business first and provide the best customer service experience with our IT Support.

Lisa H R, Workplace Matters