

The Small Business Cyber Crisis

7 Urgent And Critical Protections Every Small And Medium Sized Business Must Have In Place NOW To Protect Their Bank Accounts, Client Data, Confidential Information And Reputation From The Tsunami Of Cybercrime

Dedicated To Your Success
info@connectability.com | 647-930-2250



The Small Business Cyber Crisis

The 7 Urgent And Critical Protections Every Small And Medium Sized Business Must Have In Place NOW To Protect Their Bank Accounts, Client Data, Confidential Information And Reputation From The Tsunami Of Cybercrime

The growth and sophistication of cyber criminals, ransomware and hacker attacks has reached epic levels. CEOs can no longer ignore it or foolishly think “that won’t happen to us.”

Your business – large OR small – will be targeted and will be compromised UNLESS you take action on the information revealed in this shocking new executive report. Putting these protections in place can drastically reduce or eliminate the reputational damages, downtime, data loss, litigation, embarrassment and significant costs of a cyber-attack.

Provided By: Connectability

Author: Brad Shafran, Vice President

www.connectability.com

647-930-2250

970 Lawrence Ave W, Suite 402, Toronto

Notice: This publication is intended to provide accurate and authoritative information in regard to the subject matter covered. However, no warranties are made. It is provided with the understanding that the author and the publisher is NOT engaged in rendering legal, accounting or related professional services or advice and contains opinions of its author. This publication is NOT intended as a substitute for specific legal or accounting advice for any particular institution or individual. The publisher accepts NO responsibility or liability for any individual’s decisions or actions made as a result of information or opinion contained herein.

When You Fall Victim To A Cyber-Attack By 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, rape, mugging, carjacking, theft – get sympathy from others. They are called “victims” and support comes flooding in, as it should.

But if your business is the victim of a cybercrime attack where client data is compromised, you will **NOT** get such sympathy. You will be instantly labeled 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 adequate, you can be found liable, facing serious fines and lawsuits **EVEN IF** you trusted an outsourced IT support company to protect you. Claiming ignorance is not an acceptable defense, and this giant, expensive and reputation-destroying nightmare will land squarely on YOUR shoulders. *But it doesn't end there...*

Under Canadian law, you are required to tell your clients that YOU exposed them to cybercriminals, assuming there is a real risk of significant harm associated with the breach. Your competition will have a heyday over this. Clients will be **IRATE** and leave in droves. Morale will **TANK** and employees will **BLAME YOU**. Your bank is **NOT** required to replace funds stolen due to cybercrime (*go ask them*), and unless you have a very specific type of cyber insurance, any financial losses will be denied coverage by your general business liability policy.

Please do NOT underestimate the importance and likelihood of these threats. It is **NOT** safe to assume your IT company (or guy) is doing everything they should be doing to protect you; in fact, there is a high probability they are **NOT**, which we can demonstrate with your permission.

Yes, It CAN Happen To YOU And The Damages Are **VERY** Real

You might already know about the escalating threats, from ransomware to hackers; but it's very possible you are underestimating the risk to you. It's also possible you're **NOT** fully protected and are operating under a false sense of security, ill-advised and under-served by your outsourced IT company.

In fact, if they have not talked to you about the protections outlined in this report, or about putting a cyber “disaster recovery” plan in place, you are at risk and you are not being advised properly.

This is not a topic to be casual about. Should a breach occur, your reputation, your money, your company and your neck will be on the line, which is why you must get involved and make sure your company is prepared and adequately protected, not just pass this off to someone else.

This Is Too Serious A Matter To Entrust To Others And Delegate Without Your Involvement

This is no longer an issue that can simply be delegated to the IT department.

ONE slipup from even a smart, tenured employee clicking on the wrong email, innocently downloading an application, lazily using an easy-to-remember password for ONE application is all it takes to open the door to a hacker or ransomware **and create real damage.**

Take the story of Michael Daugherty, former CEO of LabMD. His small, 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 services 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 shared on the situation was “inadequate,” requesting in-person testimony from the staff regarding the breach, and requesting more details on what training manuals he had provided to his employees regarding cybersecurity, documentation on firewalls and penetration testing. (QUESTION: ARE YOU DOING ANY OF THIS NOW?)

Long story short, his employees blamed HIM and left, looking for more “secure” jobs at companies that weren’t under investigation. Sales steeply declined as clients took their business elsewhere. His insurance providers refused to renew their policies.

The FTC relentlessly pursued him with demands for documentation, testimonies and other information he already provided, sucking up countless hours of time. 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, storing what was left of the medical equipment he owned into his garage where it remains today (image below).



“Not My Company...Not My People...We’re Too Small” You Say?

Don’t think you’re in danger because you’re “small” and not a big company like Facebook, Capital One, J.P. Morgan or Home Depot? That you have “good” people and protections in place? That won’t happen to you?

That’s EXACTLY what cyber criminals are counting on you to believe. It makes you easy prey because you put ZERO protections in place, or grossly inadequate ones.

Look: 82,000 NEW malware threats are being released **every single day** and HALF of the cyber-attacks occurring are aimed at small businesses; you just don’t hear about it because the news wants to report on BIG breaches OR it’s kept quiet by the company for fear of attracting bad PR, lawsuits, data-breach fines and out of sheer embarrassment. But make no mistake – small, “average” businesses are being compromised daily, and clinging to 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 only the ones that were reported. Most small businesses do NOT report such losses.

Are you “too small” to be significantly damaged by a ransomware attack that locks all of your files for several days or more? Are you “too small” to deal with a hacker using your

Connectability | 970 Lawrence Ave W, Suite 402 | Toronto, ON M6A 3B6

Website: www.connectability.com | Phone: 647-930-2250

company's server as "ground zero" to infect all of your clients, vendors, employees and contacts with malware? Are you "too small" to worry about someone taking your payroll out of your bank account? According to Osterman Research, small businesses lost over \$100,000 per ransomware incident and over 25 hours of downtime. Of course, \$100,000 isn't the end of the world, is it? But are you okay to shrug this off? Take the chance?

It's NOT Just Cybercriminals Who Are The Problem

Most business owners erroneously think cybercrime is limited to hackers based in China or Russia; but the evidence is overwhelming that disgruntled employees, both of your company and your vendors, can cause significant losses due to their knowledge of your organization and access to your data and systems. What damage can they do?

- **They leave with YOUR company's files, client data and confidential information stored on personal devices**, as well as retaining access to cloud applications, such as social media sites and file-sharing sites (DropBox for example) that your IT department doesn't know about or forgets to change the password to.

In fact, according to an in-depth study conducted by Osterman Research, **69% of businesses experience data loss due to employee turnover and 87% of employee who leave take data with them**. What do they do with that information? Sell it to competitors or retain it to use at their next job.

- **Funds, inventory, trade secrets, client lists and HOURS stolen**. There are dozens of sneaky ways employees steal, and it's happening a LOT more than businesses care to admit. According to the website StatisticBrain, 75% of all employees have stolen from their employers at some point. From stealing inventory to cheque and credit card fraud, your hard-earned money can easily be stolen over time in small amounts that you never catch.

Here's the most COMMON way they steal: They waste HOURS of time on your dime to do personal errands, shop, play games, check social media feeds, gamble, read the news and a LONG list of non-work related activities. And it's only getting worse with an increasing number of businesses opting to allow employees to work from home. Of course, YOU are paying them for a 40-hour week, but you might only be getting half of that. Then they complain about being "overwhelmed" and "overworked." They tell you, "You need to hire more people!" so you do. All of this is a giant suck on profits if you allow it. Further, if your IT company is not monitoring what they do and limiting what sites they can visit, they could do things that put you in legal jeopardy, like downloading illegal music and video files, visiting adult content websites, gaming and gambling – all of these sites fall under HIGH RISK for viruses and phishing scams.

- **They DELETE everything. A common scenario:** An employee is fired or quits because they are unhappy with how they are being treated– but before they leave, they permanently

delete ALL their emails and any critical files they can get their hands on. If you don't have that data backed up properly, you lose it ALL. Even if you sue them and win, the legal costs, time wasted on the lawsuit and on recovering the data, not to mention the aggravation and distraction of dealing with it all is a far greater cost than what you *might* get awarded, *might* collect in damages.

- **Then there's the threat of vendor theft.** Your payroll, HR and accounting firm have direct access to highly confidential information and a unique ability to commit fraud. THEIR employees, not just the leadership team, can steal money, data and sell confidential information. All it takes is a part-time employee – perhaps hired to assist in data entry during tax season, and who is not being closely supervised or is working from home on routine tasks with your account – to decide to make a little money on the side by selling data or siphoning funds from your account.

Do you *really* think *this can't* happen to you?

Exactly How Can Your Company Be Damaged By A Cybercrime? Let's Count The Ways:

1. **Reputational Damages:** What's worse than a data breach? Trying to cover it up. Companies like Yahoo are learning that lesson the hard way, facing multiple class action lawsuits for NOT telling its users immediately when they discovered they were hacked. With Dark Web monitoring tools, WHERE data gets breached is easily traced so you cannot hide it anymore.

When it happens, do you think your clients will rally around you? Have sympathy? News like this travels fast on social media. They will demand answers: HAVE YOU BEEN RESPONSIBLE in putting in place the protections outlined in this report, or will you have to tell your clients, "Sorry, we got hacked because we didn't think it would happen to us," or "We didn't want to spend the money." Is *that* going to be enough to pacify them?

2. **Government Fines, Legal Fees, Lawsuits:** Breach notification statutes remain one of the most active areas of the law. Right now, the government is working to increase the fines and make legislation more aggressive, pertaining to data breaches and data privacy. If such laws are passed, it would mean mandatory controls and inspections be put in place for data privacy, with severe fines and penalties to companies that fail to comply, as well as compensation to consumers for stolen data.

Don't think for a minute that this only applies to big corporations: ANY small business that collects customer information also has important obligations to its customers to tell them if they experience a breach. In fact, the government of Canada has their own data breach and notification laws – and they are getting tougher by the minute. And if you manage financial or medical records, or your industry is regulated, your compliance requirements could be stricter.

If you're in healthcare and financial services, you have additional notification requirements under the Personal Health Information Protection Act (PHIPA), the Ontario Securities Commission (OSC) and the Investment Industry Regulatory Organization of Canada (IIROC). Among other things, PHIPA stipulates that if a healthcare business experiences a breach, **it must report the breach to the Information and Privacy Commissioner of Ontario.** The OSC and IIROC also require financial services businesses to contact them about breaches, as well as any provincial regulatory bodies.

With all the new laws being passed, there is a very good chance you are NOT compliant – what HAS your IT company told you about this?

3. **Cost, After Cost, After Cost.** ONE breach, one ransomware attack, one rogue employee can produce HOURS of extra work for staff who are already maxed out when things are going well. Then there's business interruption and downtime, backlogged work delivery for your current clients. Loss of sales. Forensics costs to determine what kind of attack occurred, what part of the network is/was affected and what data was compromised. Emergency IT restoration costs for getting you back up *if* that's even possible. In some cases, you'll be forced to pay the ransom and maybe – *just maybe* – they'll give you your data back. Then there are legal fees and the cost of legal counsel to help you respond to your clients and the media. Cash flow will be significantly disrupted, budgets blown up.

According to the Cost of Data Breach Study conducted by Ponemon Institute, the **average cost of a data breach is \$225 per record compromised, after factoring in IT recovery costs, lost revenue, downtime, legal fees, etc.** How many client records do you have? Employees? Multiply that by \$225 and you'll start to get a sense of the costs to your organization. [NOTE: Healthcare data breach costs are the highest among all sectors.]

4. **Bank Fraud.** If your bank account is accessed and funds stolen, the bank is NOT responsible for replacing those funds. Take the true story of Verne Harnish, CEO of Gazelles, Inc. a very successful and well-known consulting firm and author of the bestselling book, *The Rockefeller Habits*.

Harnish had \$400,000 taken from his bank account when hackers were able to access his PC and intercept emails between him and his assistant. The hackers, who are believed to be based in China, sent an email to his assistant asking her to wire funds to 3 different locations. It didn't seem strange to the assistant because Harnish was then involved with funding several real estate and investment ventures. The assistant responded back for confirmation, and the hackers, posing as Harnish, replied assuring her that it was to be done. The hackers also deleted his daily bank alerts, which he didn't notice because he was busy running the company, traveling and meeting with clients. That money was never recovered, and the bank is not responsible.

Everyone wants to believe, "Not MY assistant, not MY employees, not MY company" – but do you honestly believe that your staff is incapable of making a single mistake? A poor judgement? **Nobody believes they will be in a car wreck when they leave the house every day, but you still put the seat belt on.** You don't expect a life-threatening crash, but that's not a reason to not buckle up. *What if?*

Claiming ignorance is not a viable defense, nor is pointing to your outsourced IT company to blame them. YOU will be responsible, and YOUR company will bear the brunt.

5. **Using YOU As The Means To Infect Your Clients.** Some hackers don't lock your data for ransom or steal money. Instead, they use your server, website or profile to spread viruses and/or compromise other PCs. If they hack your website, they can use it to relay spam, run

malware, build SEO pages or promote their religious or political ideals. (Side note: this is why you also need advanced endpoint security, Dark Web monitoring, spam filtering, threat detection, web gateway security and the other items detailed in this report, but more on those in a minute.) Are you okay with that happening?

You May Want To Believe You're "Safe" **But Are You Sure?**

It's very possible that you are being ill-advised by your current IT company. What have they recently told you about the rising tsunami of cybercrime? Have they recently met with you to discuss new protocols, new protections and new systems you need in place TODAY to stop the NEW threats that have developed over the last few months?

If not, there could be several reasons for this. First, and most common, they might not know HOW to advise you, or even that they should. Many IT companies know how to keep a computer network running **but are completely out of their league when it comes to dealing with the advanced cyber security threats we are seeing recently.**

Second, they may be "too busy" themselves to truly be proactive with your account – or maybe they don't want to admit the service package they sold you has become OUTDATED and inadequate compared to far superior solutions available today. At industry events, I'm shocked to hear other IT companies say, "We don't want to incur that expense," when talking about new and critical cyber security tools available. Their cheapness CAN be your demise.

And finally, NOBODY (particularly IT guys) likes to admit they are out of their depth. They feel compelled to exaggerate their ability to avoid being fired. To be fair, they might actually have you covered and be on top of it all. So how do you know?

Is Your Current IT Company Doing Their Job? **Take This Quiz To Find Out**

If your current IT company does not score a "Yes" on every point, they are NOT adequately protecting you. Don't let them "convince" you otherwise and DO NOT give them a free pass on any one of these critical points.

Further, it's important that you get verification on the items listed. Simply asking, "Do you have insurance to cover US if you make a mistake?" is good but getting a copy of the policy or other verification is critical. When push comes to shove, they can deny they told you.

- ☐ **Have they met with you recently – in the last 6 months – to specifically review and discuss what they are doing NOW to protect you?** Have they told you about new and

Connectability | 970 Lawrence Ave W, Suite 402 | Toronto, ON M6A 3B6

Website: www.connectability.com | Phone: 647-930-2250

inexpensive tools such as Dark Web monitoring for your company's credentials or advanced endpoint security to protect you from attacks that antivirus is unable to detect and prevent? If you are outsourcing your IT support, they should, at a MINIMUM, provide you with a bi-yearly review and report of what they've done – and are doing – to protect you AND to discuss new threats and areas you will need to address.

- ☐ **Do they proactively monitor, patch and update your computer network's critical security settings daily? Weekly? At all? Are they reviewing your firewall's event logs for suspicious activity?** How do you know for sure? Are they providing ANY kind of verification to you or your team?
- ☐ **Have they EVER urged you to talk to your insurance company** to make sure you have the right kind of insurance to protect against fraud? Cyber liability?
- ☐ **Do THEY have adequate insurance to cover YOU if they make a mistake and your network is compromised?** Do you have a copy of THEIR CURRENT policy? Does it specifically cover YOU for losses and damages?
- ☐ **Have you been fully and frankly briefed on what to do IF you get compromised?** Have they provided you with a response plan? If not, WHY?
- ☐ Have they told you if they are outsourcing your support to a 3rd-party organization? **DO YOU KNOW WHO HAS ACCESS TO YOUR PERSONAL COMPUTER AND NETWORK?** If they are outsourcing, have they shown you what security controls they have in place to ensure a rogue technician, living in another country, would be prevented from using their free and full access to your network to do harm?
- ☐ **Do they have a ransomware-proof backup system in place?** One of the reasons the WannaCry virus was so devastating was because it was designed to find, corrupt and lock BACKUP files as well. ASK THEM TO VERIFY THIS. You might *think* you have it because that's what your IT vendor is telling you.
- ☐ **Can they offer you a complete mobile and remote device security policy, and distribute it to you and your employees?** Is the data encrypted on these devices? Do you have a remote "kill" switch that would wipe the data from a lost or stolen device, and is that data backed up so you CAN wipe the device and not lose files?
- ☐ **Do they have controls in place to force your employees to use strong passwords?** Do they require a password update be done for all employees every 3 or 6 months? If an employee is fired or quits, do they have a process in place to make sure ALL passwords are changed?
- ☐ **Have they discussed and/or implemented "multi-factor authentication" or "two-factor authentication" for access to highly sensitive data?** Do you even know what that is? If not, you don't have it.

- ☐ **Have they implemented (or offered to implement) web-filtering technology to prevent your employees from going to infected websites, or websites you DON'T want them accessing at work?** Porn and adult content is still the #1 thing searched for online. This can expose you to sexual harassment and child pornography lawsuits, ransomware, and malware - not to mention the distraction and time wasted on YOUR payroll, with YOUR company-owned equipment.
- ☐ **Have they provided you and your employees ANY kind of cyber security awareness training?** Have they offered to help you create an AUP (acceptable use policy)? How about self-paced cybersecurity training? Employees accidentally clicking on a phishing email, downloading an infected file or malicious application is still the #1-way cybercriminals hack into systems. Training your employees FREQUENTLY is one of the most important protections you can put in place. Seriously.
- ☐ **Have they properly configured your email system to prevent the sending/receiving of confidential or protected data?** Properly configured email systems can automatically prevent emails containing specified data, like social security numbers, from being sent or received. These systems can also be configured to prevent unwanted, potentially malicious emails from getting to your inbox in the first place.
- ☐ **Do they offer, or have they at least talked to you about, Dark Web/Deep Web ID monitoring?** There are new tools available that monitor cybercrime websites and data for YOUR specific credentials being sold or traded. Once detected, it notifies you immediately so you can change your password and be on high alert.

Pre-Emptive Independent Risk Assessment: The ONLY Way You Can Really Be Sure

A Security Assessment is exactly what it sounds like – it’s a process to review, evaluate and “stress test” your company’s network to uncover loopholes and vulnerabilities BEFORE a cyber event happens.

Just like a cancer screening, a good assessment can catch problems while they’re small, which means they will be a LOT less expensive to fix, less disruptive to your organization AND give you a better chance of surviving a cyber-attack.

An assessment should always be done by a qualified 3rd party, NOT your current IT team or company; fresh eyes see things hidden, even in plain sight, from those looking at it daily.

You want a qualified “Sherlock Holmes” investigating on YOUR behalf who is not trying to cover up inadequacies or make excuses, bringing to you a confidential report you can use before others find dirty laundry and air it in harmful ways.

Our Free Cyber Security Risk Assessment Will Give You The Answers You Want, The Certainty You Need

For a limited time, we are offering to give away a Free Cyber Security Risk Assessment to a select group of businesses. This is entirely free and without obligation. EVERYTHING WE FIND AND DISCUSS WILL BE STRICTLY CONFIDENTIAL.

This assessment will provide verification from a **qualified 3rd party** on whether or not your current IT company is doing everything they should to keep your computer network not only up and running, but SAFE from cybercrime.

Here’s How It Works: At no cost or obligation, one of my lead consultants and I will come to your office and conduct a non-invasive, CONFIDENTIAL investigation of your computer network, backups and security protocols. Your current IT company or guy DOES NOT NEED TO KNOW we are conducting this assessment. Your time investment is minimal: one hour for the initial meeting and one hour in the second meeting to go over our Report Of Findings.

When this Risk Assessment is complete, you will know:

- **If you and your employees’ login credentials are being sold on the Dark Web.** We will run a scan on your company, right in front of you, in the privacy of your office if you prefer (results will NOT be e-mailed or otherwise shared with anyone but you). It’s RARE that we don’t find compromised credentials – and I can guarantee what we find will shock and alarm you.

- IF your IT systems and data are **truly secured** from hackers, cybercriminals, viruses, worms and even sabotage by rogue employees.
- IF your **current backup would allow you to be back up and running again fast** if ransomware locked all your files. *In the vast majority of computer networks, we've reviewed over the years, the owners were shocked to learn the backup they had would NOT survive a ransomware attack.* Ransomware is **designed to infect your backups as well**, leaving you defenseless. There are many backup systems that cannot prevent this from happening.
- IF employees truly know how to spot a phishing email? We will actually put them to the test. *We've never seen a company pass 100%. Never.*
- Are your IT systems, backups and email settings are in sync with compliance requirements, and using best practices to find out if you can be back up and running quickly in the event of a disaster, or a hardware failure.

If we DO find problems...overlooked security loopholes, inadequate backups, credentials that have been compromised, out-of-date firewall and antivirus software and (often) active malware...on one or more of the PCs in your office, we will propose an Action Plan to remediate the situation that you can have us implement for you if you choose.

Again, I want to stress that EVERYTHING WE DISCUSS AND DISCOVER WILL BE STRICTLY CONFIDENTIAL.

Why Free?

Frankly, we want the opportunity to be your IT company. We know we are the most competent, responsive and trusted IT services provider to small businesses in the Toronto area.

However, I also realize **there's a good chance you've been burned, disappointed and frustrated by the complete lack of service and the questionable advice** you've gotten from other IT companies in the past. In fact, you might be so fed up and disgusted with being "sold" and underserved that you don't trust anyone. *I don't blame you.*

That's why this assessment is completely and entirely free. Let us earn your trust by demonstrating our expertise. While we would love the opportunity to be your IT company, we will come in with no expectations and only look to provide you with fact-based information so you can make a quality, informed decision – and we'll ONLY discuss the option of becoming your IT company if the information we share makes sense and you want to move forward. No hard sell. No gimmicks and no tricks.

Please...Do NOT Just Shrug This Off (What To Do Now)

I know you are *extremely busy* and there is enormous temptation to discard this, shrug it off, worry about it “later” or dismiss it altogether. That is, undoubtedly, the easy choice...but the easy choice is rarely the RIGHT choice. **This I can guarantee:** At some point, you WILL HAVE TO DEAL WITH A CYBER SECURITY EVENT.

Hopefully you’ll be brilliantly prepared for it and experience only a minor inconvenience at most. But if you wait and do NOTHING, I can practically guarantee this will be a far more costly, disruptive and devastating attack that will happen to your business.

You’ve spent a lifetime working hard to get where you are today. Don’t let some lowlife thief operating outside the law in another country get away with taking that from you. And certainly don’t “hope” your IT guy has you covered.

Get the facts and be certain you are protected.

Contact us and schedule your Free, CONFIDENTIAL Cyber Security Risk Assessment today: <https://www.connectability.com>. Feel free to also reach out to me direct at the phone number and email address below.

Dedicated to serving you,

Brad Shafran

Web: www.connectability.com

Email: brads@connectability.com

Phone: 647-930-2250

P.S. – When I talked to other IT professionals like myself and the CEOs who have been hacked or compromised, almost all of them told me they thought their IT guy “had things covered.” I’m also very connected with other IT firms across North America to “talk shop” and can tell you most IT guys have never had to deal with the enormity and severity of attacks happening in the last few months. That’s why it’s VERY likely your IT guy does NOT have you “covered” and you need a preemptive, independent risk assessment like the one I’m offering in this letter.

As a CEO myself, I understand that you have to delegate and trust, at some level, that your employees and vendors are doing the right thing – but it never hurts to validate that they are. Remember, it’s YOUR reputation, YOUR money, YOUR business that’s on the line. THEIR mistake is YOUR nightmare.

Here Are Just A Few Other CEOs We've Helped:

“Proactive, Reliable IT Support That Nonprofits Can Trust”

We are a small, nonprofit arts service organization and Connectability's IT support services have been of great benefit to our team. They are responsive to our needs, and we always feel comfortable reaching out because we know Connectability will be prompt and helpful in providing an effective solution. They are also proactive in identifying potential areas of improvement and suggesting IT solutions before major issues arise. Their team is professional, reliable and knowledgeable in all areas of IT support. We highly recommend their services.



Diane Davy Executive Director
Work in Culture

“Their Responsive Local IT Support Keeps our Manufacturing Operations Running Smoothly”

As a small business, we don't have the resources for a full-time IT staff, so having Connectability by our side has been a game-changer. Their team provides responsive and professional technical support exactly when we need it, without the overhead. Since we specialize in manufacturing, it's crucial for our operations to stay uninterrupted, and Connectability's local support is always available. They consistently deliver with quick response times and on-site support whenever needed. I'd absolutely recommend them for the value, service quality, and peace of mind they bring.”



Scott Jones General Manager
KB Components Toronto Inc.

“Connectability is A Trusted IT Partner That Feels Like Part of Our Own Team”

Since Connectability took over our IT, the biggest benefit has been their responsiveness. Working with them feels like having an extension of our own team—someone who not only

knows what they're doing but also guides us through challenges with confidence and expertise. What sets Connectability apart is their proactive approach to minimizing risk. They don't just react to issues; they help prevent them before they occur. Their efforts to educate our team, like weekly cybersecurity emails and simulated phishing tests, have been invaluable in reducing risks and improving our overall security. We've worked with other IT firms in the past, but Connectability is the best fit by far. Their combination of proactive guidance, effective issue resolution, and day-to-day responsiveness makes them an exceptional partner for any business.



Brian Leon CEO
Choice Hotels Canada

“Resolves Technology Issues Promptly and Competently”

The team at Connectability has provided our organization with expert IT service for the past eight years. Regardless of the size or complexity of the issue we may be facing, the staff at Connectability respond quickly and are always able to resolve our issues promptly and competently. They also provide us with expert advice on new purchases and through their relationships with manufacturers, have been able to put together custom hardware packages that meet our needs in every way.

Our organization appreciates the efforts made by Connectability to explore new products and strategies that might benefit their clients. For example we are now using their Cloud backup solution and have the added comfort of knowing our important files are always retrievable. For expert knowledge and excellent service, Connectability is definitely our number one choice.



Rae Roebuck Partner
First Leadership Limited

“In our experience of working with Connectability, we have found them to be unfailingly honest, responsive and reliable”

That level of trust has really given me the peace of mind that our IT operations are being taken care of effectively. I also feel like they really have our best interest in mind – something you don't get from every IT provider. If you have any doubts, I recommend reaching out to their CEO Ted and scheduling a call!



Michael ElmanCEO
Plastic Dress-Up Inc