Special CEO Report

The CEO's Guide To Co-Managed IT

A NEW Approach To Securing The IT Support You Need WITHOUT The Cost And Difficulty Of Hiring A Large In-House IT Department

Provided By: Connectability
Author: Ted Shafran
75 Dufflaw Road, Suite 201B

www.connectability.com
416 966 (3306)

The Dilemma

Every day, CEOs and their executive teams are faced with tough investment decisions about where to allocate their financial resources.

Some of those decisions are easier to make than others because they can be based on logical financial analysis with safe ROI expectations. Investing in marketing, a new product line, an acquisition and strategic hires all build equity and future profits. These investments are relatively safe and dependable.

However, CEOs must also deal with a new category of investments that refuse to behave typically and often don't easily secure a direct ROI. These investments involve IT, and they are growing in number, breadth and scope.

IT investments are more difficult to estimate, and the ROI or benefit might not be obvious or easily measured. In fact, you hope some NEVER produce a tangible ROI, like investing in cyber security and disaster recovery protections. However, no company can afford to lag behind in IT There's not a single department or function of your organization that isn't significantly controlled by, enhanced by, facilitated by and outright dependent on IT. And if your organization is NOT properly invested in cyber-protection and backup technologies, one cyber-attack or data-erasing event could have serious, long-lasting, costly ramifications – or even put you out of business.

But no one has unlimited funds. **So, what do you do about all of this?**

One option is to ignore it. Keep the status quo, make do with the IT staff and technology investments you have today (regardless of how old and antiquated they are) and "hope" everything is going to be okay. Trust that your current IT department has it "handled." But you have to know this is a perilous tightrope. People in New Orleans trusted the dams and levees to hold – and they did – *until* they were hit with a Category 5 hurricane.

Your Category 5 might be a ransomware attack or a rogue employee. It might be a failed server that went down, taking all its data with it, never to be revived again. It might be a corrupt SQL database that is beyond their expertise to fix. It might be an employee falling for a phishing attack, or an employee accessing bank statements from an unsecure Wi-Fi connection.

Maybe your IT department truly does have it "all covered." *Maybe.*

But if you are like most of the executives we work with to deliver co-managed IT, your IT person or department is significantly understaffed, overwhelmed and simply not able to keep up with the growing demands your company is putting on them. They also may be lacking in specialized knowledge about any number of things – data backup and disaster recovery, cyber security protections, secure cloud computing, complex database management and more.

No one IT person can do it all or know it all.

Fact is, your IT department might NOT be as prepared and capable as you may think to handle the rising complexity of IT systems for your growing company AND the overwhelming sophistication of cyber threats with the current resources, time and skill sets they have.

If true, **your organization IS AT RISK for a significant IT failure**.

To be crystal clear, I'm NOT suggesting your IT lead and staff aren't smart, dedicated, capable, hardworking people.

Fact is, NOBODY likes to go to the leadership team with "bad news" or to constantly ask for more money or help, particularly if they've already been told "there's no budget." It may be uncomfortable or even embarrassing for them to admit they don't have it all covered or that they're lagging behind, not getting things done as well as they could *because* they're just crushed with putting out fire after fire.

Further, it takes a small army to run an IT department for a company of your size and growth – and you may be unfairly expecting too much of them, setting them up for failure.

Signs That You May Be Pushing Your IT Lead And/Or Department To The Limit

For the reasons stated above, conscientious IT leaders and staff often WON'T tell you they need more money, more staff, more help. They are trying to be good stewards of your company and budget – so it's up to YOU as the leader of your organization to ensure you are not setting them up for failure or burnout.

Here are 4 early warning signs you may be pushing your IT department too hard:

1. **They're routinely working nights and weekends.** Everyone pulls an extended shift once in a while when a deadline is looming or due to a seasonal surge. But if your IT leader and department are ROUTINELY working nights and weekends to catch up, that's a sign they are understaffed, which can lead to an unhealthy workplace environment, exhaustion and burnout. It can also lead to important details being skipped and mistakes being made.

   You might not even realize this is happening, so ask them. How often are you working overtime to get things done? How caught up are you on major projects? It's not uncommon for IT staff to be stressed to the max without the leadership team even knowing about it. *This will end up hurting your organization*.

2. **Projects aren't getting done on time or correctly.** Most CEOs and CFO's aren't technically savvy, so it's difficult to know for certain if a project is taking longer than it should, or costing more than it should. All too often, a manager will jump to the conclusion that the employee is incompetent or lazy – but that may not be the case at all. It could be they're so overwhelmed with tasks and putting out fires that they can't GET the

time to do the project properly.

3. **Heightened emotional display, aggression or resentment.** Some employees will "suck it up" and push through, not wanting to talk to you about desperately needing more help. Or maybe they HAVE brought it up, only to be shut down and told "there's no money." When this happens, it's easy for an employee to become resentful. You might think that emotion and work don't mix, but your employees are only human, and will only tolerate so much.

4. **They aren't rolling out preventative security measures.** Has your IT leader rolled out any type of end-user security awareness training? Do they enforce the use of strong passwords and compel employees to change their passwords routinely? Have they tested your backups recently? Have they put together an Acceptable Use document or training to make sure employees know what is and isn't allowed with company email, Internet, confidential data, etc.? Have they given you updated documentation on the network and an up-to-date disaster recovery plan?

   All of these are essential preventative maintenance that often gets neglected or ignored when an IT person or department is overwhelmed – but these are critical for insurance purposes and reducing the chances of a cyber-attack or other disaster that would carry significant financial losses and/or hurt your company's reputation.

This May Be One Of The Biggest Dangers You Face

Without a doubt, the one area that you are most at risk for with an overwhelmed and understaffed IT department is cyber security. One incident can lead to data loss, extended downtime and (potential) liability with a cyber security breach or compliance violation.

As I stated above, the FIRST thing that gets left undone when projects loom and there are multiple fires to put out is preventative maintenance. If your employees are running into your IT team's office every 5 minutes needing a password reset or needing help getting into their email, it's hard to tell that employee "no" because they're working on server maintenance or updating critical documentation.

It's the classic "important not urgent" work that gets neglected.

To make matters worse, the complexity of knowing how to protect your organization against cybercrime and how to be in compliance with new data privacy laws is growing exponentially. These matters require SPECIALIZED knowledge and expertise. They require constant monitoring and attention. CORRECT solutions. Regardless of your organization's size or industry, these are areas you cannot ignore or be cheap about.

In situations where companies were fined or sued for a data breach, it was their WILLFUL NEGLIGENCE that landed them in hot water. They knowingly refused or failed to invest in the proper IT protections, support, protocols and expertise necessary to prevent the attack.

You'd be foolish to underestimate the cost and crippling devastation of a complete, all-encompassing systems failure or ransomware attack. You don't want to dismiss this as "It won't happen to us." And you certainly don't want to underestimate the level of expertise you need.

One innocent mistake made by an employee. One overlooked patch or update. One missed backup can produce EXTENDED downtime, data loss, and business interruptions.

Yes, your IT department is probably doing everything they can to protect you – **but it's up to YOU to be certain**. Everyone in your company – including your clients – is depending on you.

Exactly How Can Your Company Be Damaged By Failing To Invest Properly In Cybercrime Prevention And Expertise? Let Us Count The Ways:

1. **Reputational Damages:**
   When a breach happens, do you think your clients will rally around you? Have sympathy? This kind of news 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 sufficient to pacify those damaged by the breach?

2. **Government Fines, Legal Fees, Lawsuits:**
   Did you know that PIPEDA (the Personal Information Protection and Electronic Documents Act) which was enacted by Parliament in 2000 provides for penalties of **up to $100,000** for a data breach that exposes confidential customer information?

   Don't think for a minute that this applies only 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, a few provinces have their own unique data breach laws and more are on the way. Plus, these data breach laws are getting tougher by the minute.

   If you're in health care or financial services, you have additional notification requirements under the Personal Health Information Protection Act (PHIPA), the Ontario Securities Commission (OSC) and the Industry Regulatory Organization of Canada (IIROC). And if you do business in the United States or Europe, you are likely subject to privacy legislation in those jurisdictions.

   For example, New York recently passed the SHIELD Act, doubling the penalty for a data breach from $10 to $20 per failed notification and increasing the penalties from $100,000 to $250,000. No small or even midsize company can incur those costs easily. California's new

CCPA law (California Consumer Protection Act) does not require that your business reside in California, but simply that you have clients who reside there. More states are following these same paths of increased responsibility for businesses, piling on the fines, penalties and requirements for organizations to protect the data they house.

3. **Cost, After Cost, After Cost:** ONE breach, one ransomware attack, one rogue employee can create 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 hack 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, fines, 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: Health care data breach costs are the highest among all sectors.)

4. **Bank Fraud:** If your bank account is accessed and funds are stolen, the bank is NOT responsible for replacing those funds. Take the true story of Verne Harnish, CEO of the recently rebranded Scaling Up, a very successful and well-known consulting firm, and author of the best-selling 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 in the affirmative, and the hackers, posing as Harnish, assured 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 judgment? **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?*

5. **Using YOU As The Means To Infect Your Clients:**
   Some hackers don't lock your data for ransom or steal money. Often 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. Are you okay with that happening?

Do you think your IT team would never let that happen? If hackers can break into companies like Home Depot, Facebook and Capital One, they can certainly get into YOURS. The question is: Will your IT team be brilliantly prepared to minimize the damages or completely taken off guard?

Co-Managed IT: How Growth Companies Are Solving Their IT Resource Dilemma

Because GROWTH companies face the dilemma of needing professional grade IT support but can't reasonably afford to invest in all of the tools, software and staff that requires is exactly why we created a NEW solution we call co-managed IT.

In short, co-managed IT is a way for CEOs of growing companies to get the helping hands, specialized expertise and IT management and automation tools they need WITHOUT the cost and difficulty of finding, managing and retaining a large IT staff OR investing in expensive software tools.

This is NOT about taking over your IT leader's job or replacing your IT department.

It's also **NOT** a one-off project-based relationship where an IT company would limit their support to an "event" and then leave your team behind to try and support it (or give you the option to pay them big bucks afterwards to keep it working).

It's also **NOT** just monitoring your network for alarms and problems, which still leaves your IT department to scramble and fix them.

It IS a flexible partnership where we customize a set of on-going services and software tools specific to the needs of your IT person or department that fills in the gaps, supports their specific needs and gives you far superior IT support and services at a much lower cost.

Here are just a few of the reasons why CEOs of similar-sized companies are moving to a co-managed approach:

- **We don't replace your IT staff; we make them BETTER.** By filling in the gaps and assisting them, giving them best-in-class tools and training and freeing them to be more proactive and strategic, we make them FAR more productive for you. As an added bonus, THEY won't get burned out, frustrated and leave.

- **You don't have to add to your head count.** Let's face it: overhead walks on two legs. Plus, finding, hiring and retaining TOP talent is brutally difficult. With co-managed IT, you don't have the cost, overhead or risk of a big IT team and department. We don't take vacations or sick leave. You won't lose us to maternity leave or an illness, or because we

have to relocate with our spouse, or we've found a better job.

- **Your IT team gets instant access to the *same* powerful IT automation and management tools we use <u>to make them more efficient</u>.** These tools will enable them to prioritize and resolve your employees' problems faster, improve communication and make your IT department FAR more effective and efficient. These are software tools your company could not reasonably afford on its own, but they are *included* with our co-managed IT program.

- **"9-1-1" on-site**. In the unexpected event your IT leader was unable to perform their job OR if a disaster were to strike, we could instantly provide support to prevent the wheels from falling off.

- **You get a <u>TEAM</u> of smart, experienced IT pros.** No one IT person can know it all. Because you're a co-managed IT client, your IT lead will have access to a deep bench of expertise to figure out the best solution to a problem, to get advice on a situation or error they've never encountered before and to help decide what technologies are most appropriate for you (without having to do the work of investigating them ALL).

- **You'll stop worrying (or worry less!) about falling victim to a major cyber-attack, outage or data-erasing event.** We can assist your IT leader in implementing next-gen cyber security protections to prevent or significantly mitigate the damages of a ransomware attack or security breach. We can also assist in providing end-user awareness training and help you initiate controls to prevent employees from doing things that would compromise the security and integrity of your network and data. CRITICAL MAINTENANCE WILL BE DONE.

- **We provide your IT leader and team free workshops and training.** We offer quarterly webinars for our co-managed IT clients so they're more informed on critical topics such as cyber security, disaster recovery, backups, compliance regulations, best practices and more.

- **NO LONG-TERM CONTRACTS.** We're a flexible workforce you can expand and contract as needed.

Scenarios Where Co-Managed IT Just Makes Sense

Scenario 1: Your in-house IT staff is better served working on high-level strategic projects and initiatives but needs support in getting day-to-day tasks completed, such as troubleshooting various problems that arise, providing help-desk resources to your employees, software upgrades, data backup and maintenance, etc.

Scenario 2: Your in-house IT person is excellent at helpdesk and end-user support, but doesn't have the expertise in advanced cyber security protection, server maintenance, cloud technologies, compliance regulations, etc. As in scenario 1, we let them handle what they do best and fill in the

areas where they need assistance.

Scenario 3: Your company is expanding rapidly and needs to scale up IT staff and resources quickly. This is another situation where our flexible support services can be brought in to get you through this phase as you work to build your internal IT department.

Scenario 4: You have an excellent IT team, but they could be far more efficient if they had the professional-grade software tools we use to be more organized and efficient, along with our help desk. We can give them the tools, configure them for your organization and train them on how to use them. These tools will show you, the CEO, the workload they are processing and how efficient they are (we call it utilization).

Scenario 5: You have a robust in-house IT department but need on-site support and help for a remote location or branch office.

Who This Is NOT For:

Although there are a LOT of benefits to co-managed IT, this is certainly not a good fit for everyone. Here's a short list of people this won't work for.

- **Companies where the IT lead insists on viewing us as an adversary instead of an ally.** As I stated previously, our goal is not to have you fire your IT lead or your entire IT staff, but some IT managers just cannot get beyond this fear.

  As I've said, we NEED an IT-savvy leader in the company to collaborate with who knows how the company operates (workflow), understands critical applications and how they are used, company goals and priorities, etc. We cannot do that job. Co-managed IT only works when there is mutual trust and respect on both sides.

- **IT leaders who don't have an open mind to a new way of doing things.**
  Our first and foremost goal is to support YOU and your IT leader's preferences, and we certainly will be flexible – we HAVE to in order to make this work.

  However, a big value we bring to the table is our 25 years of expertise in supporting and securing computer networks. Therefore, the clients we get the best results for are ones that keep an open mind to looking at implementing our tools, methodologies and systems, and adopting some of our best practices. As I said before, this only works if it's a collaborative relationship. But we cannot – will not – take on a client that is doing things we feel compromise the integrity and security of a network, even if that's "how we've always done things" or because "that's what we like."

- **Organizations where the leadership is unwilling to invest in IT.**
  As a CEO myself, I completely understand the need to watch costs. However, starving an IT department of much-needed resources and support is foolish and risky. Further, some CEOs and CFOs look at what they are paying us and think, "We could hire a full-time

person for that money!" But they forget they are getting more than a single person – they are getting an entire team, a backup plan, tools and software, monitoring and specialized skills.

We can only help those companies that are willing to invest sufficiently in IT – not elaborately or indulgently. In fact, we can demonstrate how a co-managed IT option is a far cheaper solution than building the same team on your own.

A Cost Analysis: How Co-Managed IT Saves Your Organization Money

Below is a summary of what you get as a co-managed IT client, and what it would cost you to build it on your own.

- **Tools and Software**
  We invest considerable resources each month in software tools that our team uses to track support requests, determine utilization, monitor and maintain your network, and ensure your team is protected against the latest cyber threats. To implement these tools in your organization it would cost, at a minimum, about $1500/month. And that doesn't include the time and energy your staff would invest identifying options, testing, and finally implementing. And if they are already overworked, they might not have time to research these tools any time soon.

- **A Team of Experts**
  As I mentioned earlier, overhead walks on two legs. One of the major benefits of a co-managed IT arrangement is the fact that you have access to a team of technicians for a consistent price each month. It's hard to quantify the cost savings here because it depends on how many in-house technicians you need, but the benefit is clear: because you are working with a team instead of an individual, you can scale up and scale down as necessary. Plus, we have broad expertise with many types of technology. No need to hire a consultant any time your internal IT team doesn't have the required experience. Plus, you don't have to pay for benefits, insurance, equipment, profit sharing, vacation days or sick days.

- **Access to a Network of Consultants**
  We are a part of a network of approximately 8,000 IT consultants, MSP's and Software Developers across the US, Canada, and around the world. If we do not have expertise in a specific area, we can call upon our network to fill in the gaps. If you need a solution, we will find a vendor, vet them and manage the relationship to ensure that they complete the agreed upon project on time and within budget. No more scrambling to find a consultant on short notice with no allocated budget.

- **Cybersecurity Tools & Best Practices**
  Staying up to date on the latest vulnerabilities, threats and tactics used by hackers is no easy task. In fact, it's a full-time job. Chances are your IT lead is pulled in so many competing directions that they don't have time to invest in consistently ensuring preventive

maintenance is done each day, week and month. And if they don't have time to do preventative maintenance, then chances are they also don't have time to research the latest cyber threats and implement solutions to protect against them. A recent report by IBM and the Ponemon institute announced that the average cost of a data breach is 2020 is $3.86 million. This includes the direct and indirect costs related to time and effort in responding to a breach, lost opportunities, customer churn, bad publicity and regulatory fines. The report does go on to say that these costs are getting smaller for companies that are well prepared, however, costs are growing rapidly for businesses that don't take necessary precautions. Even if a data breach *only* costs $100,000-200,000, it can have a significant impact on cash flow, profitability, and customer retention. That's why we manage this component for our clients. There is no surefire way to prevent 100% of data breaches, but a layered approach to cybersecurity will help minimize the impact if you are ever affected.

- **Ongoing Training**
  Ongoing training is a challenge for many Internal IT teams. They may be very skilled and experienced, but due to the pace of change in technology, those skills can become outdated in a hurry. Sure, you can send them out for training, but that can be expensive. Plus, who's going to support your network while they're gone? And what happens if they leave for another company? That knowledge is gone forever. We conduct group training sessions quarterly with our Co-Managed IT customers, but we can also help train your IT staff on specific topics one on one to ensure that this knowledge exists in your organization.

- **Access to Documentation Portal & Policy Development**
  Many internal IT teams struggle to fully document the processes they follow regularly. Unfortunately, if they are sick, on vacation, or find a new job, that information disappears with them. That's one of the reasons we give all co-managed IT clients access to a cloud-based documentation portal. You now have a central repository for your policies and procedures that can be accessed from anywhere. If a member of your IT team leaves, their knowledge doesn't leave with them. Plus, we can help develop processes and procedures for your IT Department.

- **Proactive Network Monitoring & Preventative Maintenance**
  We monitor all co-managed IT environments 24/7 to identify any areas of concern like backups not running, computers that are low on disk space, and internet outages - to name a few. As a result, if you experience an issue, we often know about it right away, and can resolve it before it becomes a downtime causing misery. Since every business is different, it's difficult to predict what downtime will cost you, but a Ponemon Institute report from 2016 indicates that the cost of downtime for small businesses is between *$137 - $427 per minute*. This depends on industry, business size, and your specific operating model, but one thing is for sure: downtime is potentially toxic for client trust, and there are real financial repercussions. Based on the figures above, 1 hour of downtime costs the average small business between $8,220 and $25,620. By monitoring your network continuously, we resolve issues proactively, and before you experience downtime.

- **Preventative Maintenance**
  With so many competing priorities, preventative maintenance is often overlooked as important, but not urgent. To ensure that these activities are done every day, week and

month, we conduct regularly scheduled preventative maintenance for our Co-Managed IT clients. Our aim is to ensure that your backups, security, network and computers are in tip-top shape, and are always up to date on the latest security and feature enhancements.

- **Quarterly Business Reviews**
  While your IT lead may be very skilled and professional, how do you know that everything they say they are doing is truly getting done? Unfortunately, for a lot of Executives, the IT department is a bit of a black box. If you aren't hearing complaints from your team or your customers, then everything must be under control, right? Wrong! We regularly perform Network Assessments for businesses with internal IT teams, and we often find that preventative maintenance is not being done consistently – computers are not up to date, security patches haven't been applied, backups are running, but haven't been tested, and servers are still running old and unsupported operating systems. If you were to experience a data breach, or a hardware failure, the costs to your organization could be catastrophic. As part of our Co-Managed IT Plans, we meet with your quarterly to talk about the last 3 months, identify areas for concern, review service levels, understand more about your companies upcoming plans and how they involve technology, and discuss additional security or productivity solutions that we feel will make you more secure, efficient and effective.

We believe that, if you were to try and implement the entire structure described above, it would cost most organizations an additional $11,000 – 19,000/month – at a minimum. If you were to hire another technician to conduct preventative maintenance, and to research and implement cybersecurity solutions, the cost would be at least $5000/month ($60,000/year), not including the additional overhead. Your fully loaded costs are likely to be closer to $6500/month – and that's if you're just hiring one relatively junior technician. Under a Co-Managed IT Plan, you get more than the skills of one additional technician, you gain access to a team of senior IT experts, a collection of tools and software, monitoring, and specialized skills.

What To Look For In A Co-Managed IT Partner

As I mentioned before, other IT firms in this area will offer project-based support or monitoring only, or they want to take over IT for your entire company, firing your IT lead and/or team.

Here's why we feel these are NOT smart moves and do NOT deliver the cost savings and value for your money.

For starters, if you have a productive, reliable IT leader or department, you want to keep those people on staff, but make them more productive. No managed services provider can fully replicate the value that a full-time IT lead on your staff can deliver. They will try to sell you on that idea, but candidly, they won't be able to allocate the time and attention that a full-time employee can. As an example, we work with many customers where their IT team provides day-to-day support for end-users, desktop computers, handheld devices and peripherals. In the background, we provide monitoring and manage the networks, servers and overall infrastructure. Working together as a team, we create a seamless IT management structure.

Second, monitoring-only agreements are like smoke detectors. They tell you when a fire is about to happen (or is happening) but they don't do anything to put out the flames, get you out safe or PREVENT the fire from happening in the first place. They are a waste of money UNLESS you have a big IT team that just needs that tool – and if that's the case, you'd be better off buying that software direct, not through a reseller who will mark it up.

Finally, project-based work is often necessary, but you are going to get better results if those projects are not a "one-and-done" where they drop the solution in and take off, leaving your IT team to figure it out.

A better approach is a co-managed IT environment when a solution is implemented by the same team that is supporting it. Hand off is smoother. Underlying issues are resolved in short order. And projects are completed more quickly because the team implementing it is more knowledgeable about your technical environment.

Why We're Uniquely Positioned To Deliver Co-Managed IT

There are a number of reasons our company is uniquely positioned to be your co-managed IT partner, starting with the simple fact we're one of the few firms in the Greater Toronto Area with the depth of experience to offer it.

We are a partner you can TRUST. We're the team that will stay up into the wee hours of the night fixing a problem. We're the team you can call when an unexpected problem or crisis arises. And because we already know your environment, we can step in at any time FAST.

We are also the best Managed Services Provider in the GTA for 2018, 2019 and 2020 as named by Consumers Choice Awards. We have experience in a range of industries, so we work with a broad variety of different technologies. And because we work with so many technologies, we'll never tell you "our way or the highway". Our goal is to find you the most effective tool for your company – not to implement a one-size fits all solution. We also offer service guarantees with teeth. So, if we aren't meeting expectations, we pay for it directly. We currently serve over 45 businesses in Toronto and have a solid reputation for service built on over 25 years' experience. *But that's not all we do*. We are also a leader in cyber security – and have a thorough understand of how to protect networks from data loss, ransomware, phishing attacks, viruses, spyware, and the corresponding downtime.

I have invested tens of thousands of dollars and over 25 years in developing the most efficient, robust and responsive IT support system so you don't have to. The co-managed IT support we can wrap around you will dramatically improve your effectiveness and the quality of your IT team.

What Do Other Executives In Toronto Say?

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 Elman, Chief Executive Officer, Plastic Dress-Up Inc.

Since we started working with Connectability, they've put my worries about our technology to rest. I don't have to worry about our security, and I know that if we have issues that our IT staff can't solve, we have someone to turn to. Connectability is the first IT provider we've worked with and all I can say is that they are totally worth it for the peace of mind. They have freed up our IT staff so they can focus on the programming work which supports our clients and operations.

- Liz Gayford, Chief Financial Officer, Creative Outdoor Advertising

Think Co-Managed IT Is Right For You? Our Free Diagnostic Consultation Will Give You The Answer

If this letter struck a chord and you want to explore how (if?) a co-managed IT relationship would benefit your organization, we've reserved initial telephone appointment times with our most senior leadership team to evaluate your specific situation and recommend the co-managed IT approach that would work best based on your specific needs, budget and goals.

We work with your IT lead to determine areas that are lacking to unearth potential problems such as 1) inadequate or outdated cyber security protocols and protections, 2) insufficient backups, 3) unknown compliance violations, 4) workloads that can be automated and streamlined for cost savings and more efficiency, and 5) insufficient (or no) documentation of IT systems and assets.

These are just a few of the most frequently discovered problems we find that virtually everyone denies could exist in their organization.

We can also answer questions you might have such as:

- **Is my IT person or team 100% utilized, efficient and as productive as they should be?** We have professional tools that will give you visibility into their activities and allow you to track time against work, as well as how efficiently they are performing their job, what activities they are spending the most time on and whether or not they are maxed out, based on tangible data.

- Do you have sufficient redundancy and documented systems and processes in your IT department to avoid a single point of failure?

- Are you overspending and not getting your money's worth in any aspect of IT?

- Are you TRULY prepared and protected against a ransomware attack or other cyber security breach? Could you recover quickly? Are you meeting compliance regulations?

The above is NOT designed to make your IT team look bad; as we all know, fresh eyes see new things. They also are very unlikely to have the software tools we can provide that would give them insights and help them be FAR more effective for you. All of this will be discussed during this consultation.

To request this consultation:

1. Go online to: www.connectability.com/consult

2. Call us direct at 416-966-3306.

3. Email your appointment request to Abarnaa Arunaruban at Abarnaaa@connectability.com

One Important Request

We STRONGLY encourage you bring your IT lead into this Diagnostic Consultation so they can discuss where they feel they need the most help, and where your IT department is underutilized.

Even if you prefer we work with your IT leader direct, I also urge you to be involved. I realize that IT is not something you might fully understand, and that you are up to your neck in critical projects and deadlines – but decisions about allocating resources and budget DO require your approval and attention.

Therefore, please note that we are happy to conduct a diagnostic evaluation working mostly with your IT lead but would request you be involved, at some level, in looking at what we discover and propose.

We look forward to working with you and your team.

Sincerely,

Ted Shafran,
President
Connectability

P.S. If you would like to speak with any of our CEO clients who are utilizing our co-managed IT services, please email me at teds@connectability.com or call me at 416-966-3306 and I'll arrange for you to speak with them direct.

