



# The I.T. Leader's Guide To Co-Managed I.T.

**A NEW and NECESSARY approach to running a Top-Level I.T. Department that enables you to deliver strategic value, supreme cyber security protection and excellence in I.T. Service.**

Provided by: ITCON, INC.

[www.itconinc.com](http://www.itconinc.com)  
845.738.1661



**ItCon**  
IT & Cybersecurity Managed Services

# A Personal Letter From One I.T. Pro To Another

**FROM THE DESK OF: LEAH FREIMAN  
CEO, ITCON INC.**

Dear Fellow "Geek,"

My name is Leah Freiman. My company, ItCon Inc., specializes in delivering I.T. support and services to businesses in New York, New Jersey and Connecticut. Yes, I'm a certified geek. My love for technology started . We've been providing IT services to businesses in the New York, New Jersey and Connecticut area for over 18 years now. You may not have heard of us before, but I'm sure you're familiar with one or more of the other medical practices who are clients of ours. A few of their comments are enclosed.

Because I truly understand the unique challenges of the I.T. leader of an organization, we've developed a unique co-managed I.T. service that is designed to truly allow you to shine. This report will talk in depth about what it is and how it can help you.

After all, we both know that in MOST organizations, I.T. is the most underappreciated and misunderstood function. Think about it: when was the last time you saw an I.T. person get "employee of the month" or make the cover of a magazine? The CEOs and C-suite of companies get interviewed and talked about on podcasts and TV shows. The sales team is showered with spiffs and bonuses and freebies. The marketing team gets BIG bonuses, recognition and awards for a winning campaign, as well as BIG budgets to spend. Even the administrative assistants get appreciation, gifts and flowers. But I.T.? It's like we don't even exist.

Yet NONE of these departments could operate without reliable, secure I.T.

This is one of the reasons why I'm so passionate about being a champion to the amazing I.T. leaders we currently have the privilege to call our clients under the co-managed I.T. program. It's also why we invest a lot of time and money into free workshops and educational events for I.T. leaders in our community.

Hopefully, after reading this report, you'll consider working with us. But if not, we are still here to help you, answer questions and provide a second option on any project or problem you're currently facing.

Dedicated to your success,

*Leah Freiman*



# A Growing Crisis For I.T. Leaders

**You are charged** and held responsible for ensuring your I.T. systems are always up, running and secure so there's zero downtime, zero data loss and zero security breaches – and you're good at it. You perform admirably under the incessant, relentless pressure and crushing workload put upon you, often without sufficient resources.

A *miracle* worker.

**But the best captain sailing the high seas can't win against a tsunami's tidal wave – an unexpected, overwhelming event – and there's a very good chance you ARE going to be faced with one, unprepared.**

Let's talk candidly. Very few people truly understand the daily life of an I.T. leader...

The incredibly LONG hours, crushing workload, millions of tiny details you need to pay attention to, constant complaints and problems crossing your desk, new projects cropping up, escalating cyber security threats, new technologies you need to learn, difficult end users who refuse to follow your recommendations, much-needed maintenance looming and impossible deadlines and URGENCY on EVERYTHING.

**Even the most seasoned IT pros struggle to keep up with it all.**

To make matters worse, you're expected to operate on a shoestring budget, without sufficient staff, tools or training, forcing you to constantly choose between putting out a fire OR working on a much-needed, more strategic project you know is necessary.

## IF NOTHING HAPPENS, YOU'RE GOOD; HOWEVER...

If ONE thing goes wrong...ONE mistake, ONE oversight, ONE important detail overlooked by accident...and your organization ends up compromised by an EXPENSIVE ransomware attack or other data-erasing event resulting in extended downtime, compliance violations, business interruption, lost sales and customer trust, the epicenter will be in your office. They'll be lined up at your door with questions about what you did to prevent this from happening, and **potentially** looking to lay the blame at your feet.

**You already might realize this.** Maybe you've warned the executive team of such threats and have asked for more resources, more budget for upgrades, more staff and more tools to prevent a cyber-attack or data-erasing event from happening – and maybe you've been told time and time again there's no budget.

It's the ultimate dilemma: **You have the RESPONSIBILITY but not the ABILITY because you have NOT been given the resources, time or budget to fix it.** You need help! Unless your management team is extremely understanding, you could be in a no-win situation where your hard work, your reputation and possibly even your career are placed in peril when such an event happens.

### **So, what do you do about all of this?**

**One option is to ignore it.** Keep the status quo, make do with the staff, in-house expertise and technology you have today (regardless of how old and antiquated they are) and "hope" everything is going to be okay. Assume you have 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 your expertise to fix.

- 1. A compromised Microsoft 365 account.** A cybercriminal gains access to an employee's email account and begins sending fraudulent wire transfer requests to customers, vendors, or internal staff. What starts as a single compromised password quickly becomes a company-wide crisis.
- 2. A critical firewall or network failure.** A core piece of network infrastructure fails unexpectedly, preventing employees from accessing systems, cloud applications, email, or the Internet. Business operations grind to a halt while everyone waits for a resolution.
- 3. A ransomware attack.** I remember one IT leader who was nearly fired after a ransomware attack encrypted several critical systems. Management initially blamed him for the incident, but after a closer look, it became clear that he had repeatedly requested additional cybersecurity resources and support. The problem wasn't incompetence; it was that one person was expected to manage helpdesk tickets, projects, infrastructure, security, vendor relationships, and strategic planning all at the same time.
- 4. A failed server combined with failed backups.** Another company we now provide co-managed IT services for originally brought us in after their primary server crashed and could not be recovered. To make matters worse, their backups had silently failed months earlier, and nobody knew it. Their lone IT manager had been juggling dozens of projects, supporting hundreds of users, and constantly responding to emergencies. Routine backup verification simply fell through the cracks.
- 5. A key IT employee unexpectedly leaves.** Whether due to resignation, illness, retirement, or personal circumstances, the departure of a single IT leader can leave an organization exposed if that person was the only one who understood critical systems, vendor relationships, passwords, configurations, and recovery procedures. Suddenly, the company finds itself scrambling to maintain operations while trying to replace years of institutional knowledge.

In every one of these situations, the underlying problem is often the same: too much responsibility placed on too few people. When capable IT professionals are stretched beyond their limits, critical tasks get delayed, preventive maintenance gets skipped, and risks begin to accumulate. That's why smart organizations invest in additional expertise and support before a Category 5 event occurs—not after.

## THIS MAY BE GOING ON IN OTHER I.T. DEPARTMENTS, BUT NOT IN MINE

Maybe you have it “all covered.” But that's a BIG “*maybe*” to assume.

The I.T. department of a company that is growing – or simply opening new locations, offshoring work, allowing employees to work remote in this “everything connected” world with multiple devices, multiple users who have the ability to make mistakes and the growing sophistication of cyber-attacks – makes for a VERY complex organism.

**How can one I.T. person or even a small team of I.T. professionals protect a company with hundreds or thousands of users?** You can't *reasonably* be expected to monitor every device, every individual, every “event,” every application connected to your network. You can't possibly begin to have all the expertise you need under one roof because of the cost. You can't possibly have the TIME to stay on top of the dozens of events happening every day, especially without sophisticated monitoring tools and software (we know, because that's ALL we do every day for our clients, and we can tell you it takes an army to make it all work).

You may want to believe you have 20/20 vision into everything that is going on, but since 2008, I have not failed to find security loopholes and I.T. failures in every business we have been asked to evaluate. ***Not once.***

### **No one I.T. person can do it all or know it all.**

Fact is, you and/or your I.T. department might NOT be as prepared and capable as you may think to handle the rising complexity of I.T. systems for your growing company AND the overwhelming sophistication of cyberthreats with the current resources, time and skill sets they have. If that's true, your organization **IS AT RISK for a significant I.T. failure or cyber-attack.**

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

As I've said repeatedly, the I.T. leader's responsibilities and requirements have rapidly multiplied over the last few years due to three things:

1. The growing dependency on I.T. for ALL businesses and the growing number of devices connected to your network.
2. The exponential growth of the number of cyber-attacks and sophistication of these threats.

3. Growing compliance regulations, making the cost of a breach or cyber-incident go up exponentially, with fines, penalties, reputational damage and more.

We've already seen multiple companies get slammed with sizable fines and settlements for security incidents that were due to lax security protocols, mistakes and cover-ups. Do you really want this to happen to YOUR company on YOUR watch?

## THIS MAY BE ONE OF THE BIGGEST DANGERS YOU FACE

**Without a doubt, the areas you are most at risk for with an overwhelmed and understaffed I.T. department are data loss, extended downtime and (potential) liability with a cyber security breach or compliance violation.**

One of the FIRST things that gets left undone when urgent end-user problems pile up is preventative maintenance. If your employees are running into your office and/or your I.T. team's office every 5 minutes needing a password reset or help getting e-mail, it's hard to tell that employee "no" because they're working on server maintenance or reviewing security alerts and patching PCs to ensure your network is protected.

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 be in compliance with new data privacy laws is growing exponentially. These matters require SPECIALIZED knowledge and expertise and for your I.T. team to conduct ongoing training and refreshing of skills. 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 I.T. 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, business interruptions.

**I'm sure you're doing everything you know to do to protect your organization – but is it enough?**

The sooner you can bring us in as your ally to focus exclusively on these matters and ensure there are no oversights, no mistakes, no missteps, the more it is a mark of responsible leadership whose credit is due and justifiably earned.

# Overexaggerated Hype?

## LET US COUNT THE WAYS YOUR ORGANIZATION WILL BE AFFECTED BY AN I.T. FAILURE OR CYBER-INCIDENT:

### 1. Reputational Damages:

When a breach happens, do you think your clients/patients 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 you should, or will you have to tell your clients, "Sorry, we got hacked because we didn't think it would happen to us," or "We thought we had it handled." Is *that* going to be sufficient to pacify those damaged by the breach?

### 2. Government Fines, Legal Fees, Lawsuits:

Breach notification statutes remain one of the most active areas of the law. Right now, several senators are lobbying for "massive and mandatory" fines and more aggressive legislation pertaining to data breaches and data privacy. Multiple states are putting in place data breach notification and privacy laws that REQUIRE even small companies (and certainly larger organizations) to increase the steps they are taking to protect data they hold.

The courts are NOT in your favor if you expose client or patient data to cybercriminals.

**Don't think for a minute that this applies only to large hospital systems:** ANY medical practice, clinic, or healthcare organization that collects, stores, or transmits patient information has serious legal and ethical obligations to protect that data. Under HIPAA and related state regulations, healthcare providers are required to notify patients and regulators in the event of a breach involving protected health information (PHI). These requirements are strict, time-sensitive, and come with significant penalties for non-compliance. On top of federal rules, many states also have their own healthcare privacy and breach notification laws—and enforcement is becoming increasingly aggressive.

If you're in health care or financial services, you have additional notification requirements under the Health Insurance Portability and Accountability Act (HIPAA), the Securities and Exchange Commission (SEC) and the Financial Industry Regulatory Authority (FINRA). Among other things, HIPAA stipulates that if a health care business experiences a breach involving more than 500 customers, **it must notify a prominent media outlet about the incident**. The SEC and FINRA also require financial services businesses to contact them about breaches, as well as any state regulating bodies.

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 I.T. 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. Some states require companies to provide one year of credit-monitoring services to consumers affected by a data breach, and more are following suit.

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 I.T. 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 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 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 e-mails between him and his assistant. The hackers, who are believed to be based in China, sent an e-mail 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 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 I.T. team would never let that happen? If hackers can break into companies like First American, Facebook and Capital One, they can certainly get into YOURS. The question is: Will your I.T. team be brilliantly prepared to minimize the damages, or completely taken off guard?

## CO-MANAGED I.T.:

# How Smart I.T. Leaders Are Addressing Their Resource Dilemma

This is **EXACTLY** why we've innovated a new concept called "co-managed I.T." to provide I.T. leaders like you an escape route – a solution – that is 1) reliably effective to ensure your organization is prepared, 2) affordable, and 3) customized to YOUR specifications, YOUR needs.

In short, co-managed I.T. is a way for CIOs and I.T. leaders of growing companies to fill in the gaps and get the helping hands, specialized expertise and automation tools they need WITHOUT the cost and difficulty of finding, managing and retaining a large I.T. staff OR outright buying expensive software tools that we give you as part of our program.

**This is NOT** about taking over your job or replacing your I.T. department.

It's also **NOT** a one-off project-based relationship where an I.T. company would limit their support to an "event" or project and then leave you and 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 you responsible for scrambling and fixing the issues.

It IS a flexible partnership where we customize a set of ongoing services and software tools specific to YOUR needs that fill in the gaps, free you to be more strategic, allowing YOU to be a true I.T. leader in your organization.

Here are just a few of the reasons why I.T. leaders are moving to a co-managed approach:

- **You maintain COMPLETE control over your I.T. department and decide what you and your team will handle and what problems get passed on or escalated to us.**

All of our partnerships with current I.T. leaders are customized to YOUR specific situation, so you KEEP the workload you want and offload tasks and projects you either don't have time to do, don't want to do or simply don't have the skill set in-house to complete.

- **You get instant access to the same powerful automation and management tools we use to make your job EASIER.** We'll give you our professional-grade management tools that will allow you to capture, organize and prioritize end-user "tickets" (problems), improve communication, shorten resolution time, track software licenses and renewals, create and manage projects, document the devices



on your network and be 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 I.T. program – and we configure them, upgrade them and **train you on their use**.

- **You'll become more valuable to your organization.** Our team will free you up to work on more strategic projects and focus on YOUR strengths. You'll finally get the time to work on that long list of projects you've been wanting to get to but couldn't – or simply delegate them to us.
- **You get a TEAM of smart, experienced I.T. pros to collaborate with.** We're always here to help you figure out the best solution to a problem, get advice on a situation or error you've never encountered before or 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 you 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.
- **Access to free workshops and on-demand training.** We provide monthly workshops/training and webinars for our co-managed I.T. clients on topics ranging from cyber security to backups, etc.,. This is FREE to you and a huge value add.
- **One BIG, final benefit: You can *finally* take a vacation or a day off without everything collapsing.** You'll have a **flexible** workforce of experienced I.T. pros at the ready to assist with special projects, migrations and new technologies – or to simply give you the ability to take some time off. We are your backup I.T. team!

## WHO THIS IS NOT FOR:

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

- **I.T. leaders who insist on viewing us as an adversary instead of an ally.**  
To be clear, we do not want your job, nor will we encourage your CEO to fire you. We NEED an I.T.-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 I.T. only works when there is mutual trust and respect on both sides.



- **I.T. 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 preferences, and we certainly will be flexible. However, a big value we bring to the table is our 18 years of expertise in supporting and securing computer networks. Therefore, the clients we get the best results for are those 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.

- **Organizations where the leadership is unwilling to invest in I.T.**

As a CEO myself, I completely understand the need to watch costs. However, starving an I.T. department of much-needed resources and support is foolish and risky. Further, some CEOs 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 I.T. – not elaborately or indulgently. In fact, we can demonstrate how a co-managed I.T. option is a far cheaper solution than building the same team on your own.

## SCENARIOS WHERE CO-MANAGED I.T. JUST MAKES SENSE

**SCENARIO 1:** You are a higher-level I.T. pro who cannot get to more strategic projects because you're buried with putting out fires and other urgent needs, such as troubleshooting an endless number of end-user problems that arise, adding and removing users, ordering equipment, doing basic maintenance and more. In this scenario, our team can provide help-desk support and take that off your plate, freeing you up to work on more strategic initiatives to make your entire organization more secure, more efficient and more competitive.

**SCENARIO 2:** You or your I.T. team are excellent at helpdesk and end-user support but don't have the expertise in advanced cyber security protection, server maintenance, cloud technologies, compliance regulations, etc. As in Scenario 1, we let YOU handle what YOU do best and fill in the areas where you need assistance.

**SCENARIO 3:** A company is in rapid expansion and needs to scale up I.T. 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 I.T. department.



**SCENARIO 4:** The quantity of end users and issues you're dealing with has escalated, and you're struggling to get their requests and needs organized and prioritized. You recognize that you could be far more efficient if you had professional-grade software tools to track, organize, categorize and prioritize end-user problems, tasks, upgrades, etc. We can give you those tools, configure them for your organization and train you on how to use them. These tools will also allow you to show the CEO and executive the workload you are processing and how efficient you are (we call it utilization). After all, how many executives truly know how much you actually handle on a day-to-day basis? We can help you reveal that to them.

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

## WHAT TO LOOK FOR IN A CO-MANAGED I.T. PARTNER

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

Here's why we feel these are NOT smart moves and do NOT deliver the cost savings and value promised. Let's start with the concept of replacing you and your I.T. team.

**For starters, no MSP (managed services provider) or I.T. services company can fully replicate the value that a full-time I.T. leader has.** They will try to sell the CEO and CFO on that idea, promising incredible cost savings, but candidly, the MSP won't be able to allocate the time and attention that a full-time employee can – and if they do, the costs will absolutely be higher because they need to make a 60% to 70% margin on services. **Outsourcing only makes sense in scenarios when a FULL-TIME person is not needed**, or where there are very specialized skills needed that are difficult to find and (again) not needed on a full-time basis.

**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 I.T. team that just needs THAT specific tool – and if that's the case, then 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 you and your I.T. team to figure it out.**

A better approach is a co-managed I.T. environment where a solution is implemented WITH you by the same team that is supporting it.

# WHY WE'RE UNIQUELY POSITIONED TO DELIVER CO-MANAGED I.T.

There are a number of reasons our company is uniquely positioned to be your co-managed I.T. partner, starting with the simple fact we're the **ONLY I.T. firm in New York, New Jersey and Connecticut** specializing in 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 in a crisis or when extra hands are needed.

We are also a leader in efficient, responsive I.T. services and support, known for delivering fast response times, practical solutions, and a proactive approach that keeps businesses running without disruption. Our team brings deep real-world experience supporting complex IT environments across multiple industries, backed by years of hands-on problem-solving, system design, and infrastructure management. We've built our reputation not on theory, but on execution—showing up when it matters, resolving issues quickly, and helping organizations turn IT from a constant frustration into a reliable business asset.

We currently serve over hundreds businesses in New York, New Jersey and Connecticut and have a solid reputation for service built on over 18 years' experience. But that's not all we do. We are also recognized as leading experts in cybersecurity—second to none in our thorough understanding of how to protect networks from data loss, ransomware, business email compromise, and evolving cloud-based threats. Our approach is proactive, layered, and designed to reduce risk before incidents occur, not just respond after the damage is done.

I have invested thousands of dollars and over 18 years into developing the most efficient, robust and responsive I.T. support system so you don't have to. The co-managed I.T. support we can wrap around you will dramatically improve your effectiveness and free you up to be more strategic and valuable to your organization.



# WHAT DO OTHER I.T. LEADERS IN NY, NJ AND CT SAY?

- **ITCON IS MY IT  
AND CYBER SECURITY DEPARTMENT!**

I need to ensure that I provide my team with a reliable IT network and technical support which allows them to do their job with minimum downtime. So, when our IT and cyber security solutions weren't working, I was looking for an IT and cyber security provider and hired ItCon. ItCon did not just provide us with a product or service, they gave me an IT and cyber security department. I trust the guidance I get from Leah and the team, and this allows me to add value to the business in other areas. I see ItCon as my IT Department and therefore trust is a high factor in our relationship, I feel confident that I don't have to question their guidance. Businesses are made up of people, and the people keep the clients. We are continually called by competitors to ItCon and the key reason I don't entertain them is because we work well with the individuals within ItCon. My team feels comfortable with their team, and this makes a difference. I feel they take the smallest project (installing a printer) just as seriously as the larger ones like setting up a new office. If you haven't met anyone from ItCon yet, I'd suggest you meet them. I confidently say that ItCon supports and works in close relationship with my business. Relationships are key and are developed through time. IT companies can all sound the same, it's only when you test the service and interact with the people that you see the difference. Give ItCon a ring today.

*Milton Berg*

CEO  
MB Advisors



- **PERSONALIZED IT  
& RELIABLE TEAM!**

Before using ItCon we constantly held up with IT frustrations and had to be constantly involved with the IT of our company. ItCon came in, gave us a detailed plan customized to all our needs and is working together with our in-house IT team to always be up to par. ItCon is true to their word and has great open communication through every step. This makes me feel confident that our IT department is productive and in great hands, which gives me peace of mind. When asked if a company should hire ItCon I have 3 words for them: JUST DO IT!

*Joseph Deutsch*

CEO  
ODA Primary

- **SECURE PROACTIVE IT  
& CYBER SECURITY**

ItCon has upgraded our company to perform better, they are here for us not only to handle our IT, Cyber Security, and anything related to our data, they are ALWAYS here for us no matter how big or small the task is. With ItCon, EVERYTHING is possible! ItCon are proactive as opposed to reactive and have an excellent personal relationship with everyone in the company from executives to the people behind the phones alike. I can truly rely on them to treat my company with the utmost care while keeping it up to par and secure. If someone is shopping for a solid IT MSSP, I would tell them: Don't waste your time going around trying other firms and wasting money, time, and resources just to realize you would have saved all that and a lot of aggravation by making the right decision. Instead use that wasted money and time to help a brother in need.

*Gershon Sabol*

CEO  
Yedei Chesed



# Think Co-Managed I.T. Is Right For You?

## OUR FREE DIAGNOSTIC CONSULTATION WILL GIVE YOU THE ANSWER

If this letter has struck a chord and you want to explore how (if?) a co-managed I.T. relationship would benefit you and your I.T. department, we've reserved initial telephone appointment times with our most senior consultants to evaluate your specific situation and recommend the co-managed I.T. approach that would work best based on your specific needs, budget and goals.

We'll work with you to help you determine areas that are lacking to unearth potential problems such as 1) inadequate or outdated cyber security protocols and protections, 2) insufficient backups, 3) unrealized compliance violations, 4) workloads that can be automated and streamlined for cost savings and more efficiency, and 5) insufficient (or no) documentation of I.T. systems and assets.

These are just a few of the most frequently discovered problems we find that virtually every I.T. leader is unaware of.

Further, many I.T. leaders appreciate having fresh eyes to see things they don't, and to discover tools, methodologies and services that will make them FAR more effective and efficient – tools they don't have at their disposal and may not even know exist. All of this will be discussed during your consultation.

You can schedule your Diagnostic Consultation 3 ways:

1. Go online to: <https://www.itconinc.com/discoverycall/>
2. Call us direct at 845.738.1661
3. E-mail your appointment request to <https://www.itconinc.com/contact/>



# One Important Request

We strongly encourage you bring your CEO/CFO into this Diagnostic Consultation earlier rather than later, especially if they will need to be brought "on board" with this concept. In most cases, they are the ones giving the financial approval and therefore will have questions about us and, at a minimum, what they are being asked to invest in.

Perhaps your CEO/CFO is different and is in full agreement with you that you are understaffed and overwhelmed and in need of additional expertise, resources, tools and support. But if they are not, we can work on your behalf to help them understand the value of I.T. and the importance of proactive maintenance and specialized expertise for backups, disaster recovery and cyber security.

Of course, we will be working with you, on your behalf, to conduct the technical evaluation of your systems, security, backups, disaster recovery, licensing issues and more, and prioritize where we can be of most value to you. We look forward to working with you and your team.

*Leah Freiman*

CEO  
ItCon Inc.

P.S. If you would like to speak with any of the I.T. leaders who are utilizing our co-managed I.T. services, please e-mail me at [info@itconinc.com](mailto:info@itconinc.com) or call me at 845-738-1661 and I'll arrange for you to speak with them direct.

