

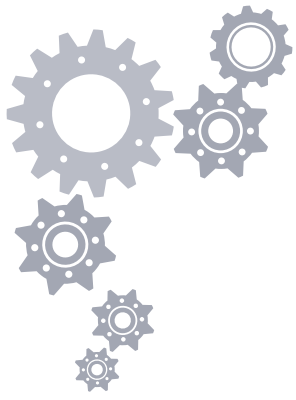
SPECIAL I.T. MANAGEMENT REPORT

# 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: Hodgson Consulting & Solutions  
Author: Robert Zehnder, President  
1110 W. Lake Cook Rd, Suite 235  
Buffalo Grove, IL 60089  
[www.hodgsonconsulting.com](http://www.hodgsonconsulting.com)  
847-906-5005



# TABLE OF CONTENTS

- 1** A Growing Crisis For IT Leaders
- 2** IF Nothing Happens, You're Good; However...
- 3** This May Be Going On In Other I.T. Departments, But Not In Mine
- 4** This May Be One Of The Biggest Dangers You Face
- 5** Over exaggerated Hype? Let Us Count The Ways Your Organization Will Be Affected By An I.T. Failure Or Cyber-Incident:
- 6** Co-Managed I.T.: How Smart I.T. Leaders Are Addressing Their Resource Dilemma
- 7** Who This Is NOT For:
- 8** Scenarios Where Co-Managed I.T. Just Makes Sense
- 9** What To Look For In A Co-Managed I.T. Partner
- 10** Why We're Uniquely Positioned To Deliver Co-Managed I.T.
- 11** Think Co-Managed I.T is Right For You? Our Free Diagnostic Consultation Will Give You The Answer
- 12** One Important Request



# 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.

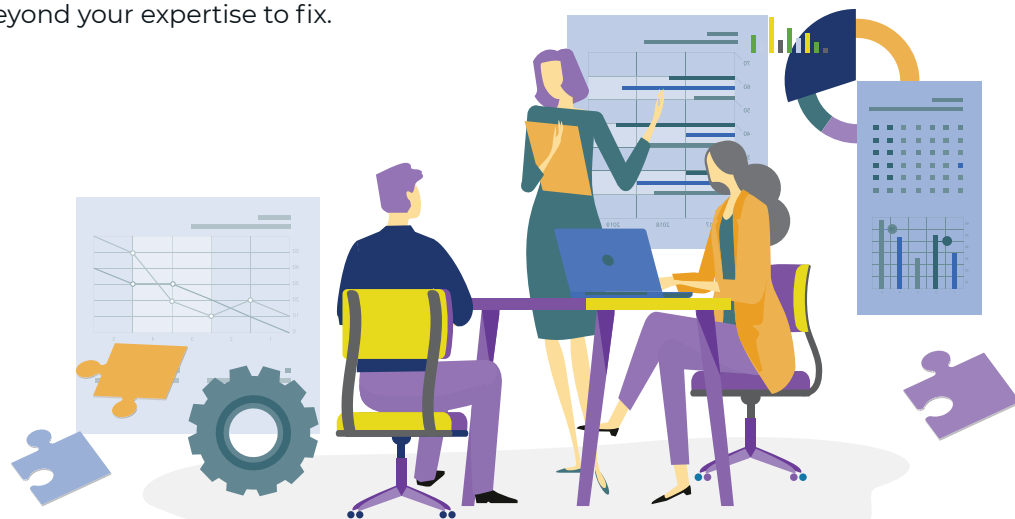
It's the ultimate dilemma: **You have the RESPONSIBILITY but not the ABILITY because you do not have the resources, time or budget to fix it.** You need help! Unless your management team is extremely understanding, you could be in a no-win situation where your hard work, your reputation and possibly 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 ransom ware 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.

For Example - A company originally brought us in when their server crashed and was unable to be revived, and their backups hadn't been functioning for 8 months. Admittedly, the I.T. leader had not been monitoring them as he should because he was up to his eyeballs in projects and other urgent matters. Was it his fault? I say no – his leadership team should have recognized he was too overwhelmed to handle everything. HIS only fault was not pushing harder with his management team on the issue of bringing in outside help.



# 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 2000, 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 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, 47 states and the District of Columbia each have their own data breach laws – and those laws are getting tougher by the minute.

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,**

**finer, 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 cybersecurity 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 workshops and webinars for our co-managed I.T. clients on topics ranging from cyber security to backups. 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 20 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.

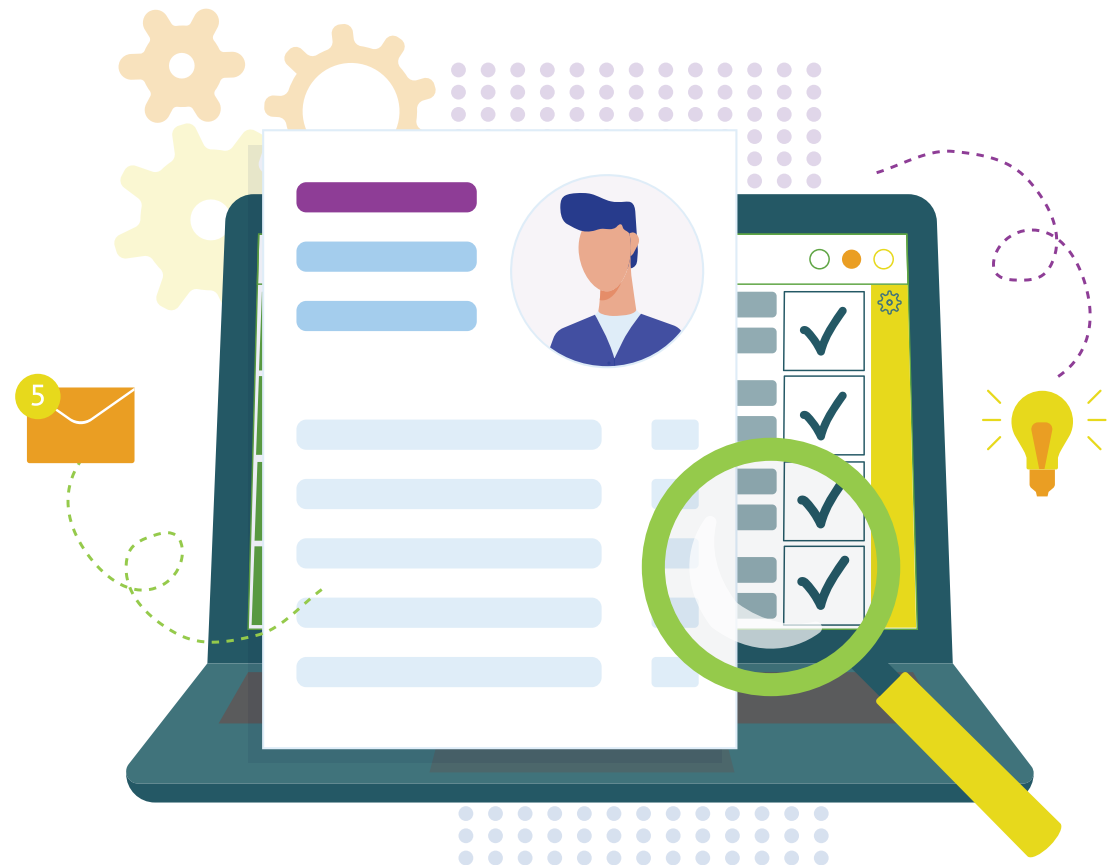
Here's why we feel these are NOT smart moves and do NOT deliver the cost savings and value promised. Let's start with the concept of replacing you and your I.T. team.

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. 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 Buffalo Grove 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 the leader in efficient, responsive I.T. services and support; we own our own US based data-center, environment, and we thrive in companies with multiple locations and/or a remote workforce. We currently serve over many businesses in the Chicagoland area and have a solid reputation for service built on over 20 years' experience. But that's not all we do. We are also the leading/preeminent experts in cyber security – second to none in our thorough understanding of how to protect networks from data loss, ransom ware and cloud technologies.

I have invested thousands of dollars and over 20 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.



# THINK CO-MANAGED IT 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: [www.hodgsonconsulting.com/itconsult](http://www.hodgsonconsulting.com/itconsult)
2. Call us direct at 847-906-5005.



# 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.

Robert Zehnder,  
President  
Hodgson Consulting & Solutions

P.S. If you would like to speak with any of the I.T. leaders who are utilizing our co-managed I.T. services, reach out to me at 847-906-5005 and I'll arrange for you to speak with them direct.

