Special Business Executive Report

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

A Far Superior Approach To Lowering The Risk, Difficulty, and Cost Of I.T. Support For Your Growing Small Or Midsize Organization

Provided By: USM Technology
Author: Stephen Cracknell
202 South Austin Drive Allen, TX 75013

www.usmtechnology.com/co-mit
214-390-9252

The Dilemma: The Rising Costs Of I.T. And Cybersecurity

Every day, business owners and their executive teams face tough investment decisions about where to allocate their financial resources.

Some decisions are easier 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 build equity and future profits. These investments are relatively safe and dependable.

However, business owners 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 I.T. (which we'll define as all aspects of information technology, data protection, security, and compliance). They are growing in number, breadth, and scope – and over the last decade, have been steadily increasing at an exponential rate as cybercrime rages, compliance regulations are introduced, and I.T. talent continues to be in short supply.

As you know, I.T. investments are more difficult to estimate, and the ROI or benefit might not be obvious or easily measured. In fact, you hope some investments NEVER produce a tangible ROI, like those in cybersecurity and disaster recovery protections. However, no company can afford to lag behind in I.T. There's not a single department or function of your organization that isn't significantly controlled by, enhanced by, or facilitated by an outright dependent on I.T.

Further, if your organization is NOT properly invested in cyber-protection and backup technologies, a single cyber-attack or data-erasing event could have serious, long-lasting, costly ramifications – or even put you out of business. Today, insurance providers are putting stricter requirements on all companies to get simple cyber liability, crime, or other policies covering the costs of a data breach or hack that severely impacts the 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 I.T. staff and technology investments you have today (regardless of how old and antiquated they are), and "hope" everything will be okay. Trust that your current I.T. department or individual "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 that locks your entire company's data down, inaccessible even from your backup. It could be a rogue employee who intentionally sabotages your organization by deleting data or selling it to a competitor. 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 current I.T. team's expertise to fix.

Maybe your I.T. department indeed does "have it all covered." *Maybe*.

But if you are like most of the business owners we work with to deliver Co-Managed I.T., then your I.T. person or department most likely is significantly understaffed, overwhelmed, and simply not able to keep up with the growing demands your company is putting on them. They also may

lack specialized knowledge about data backup and disaster recovery, cybersecurity protections, secure cloud computing, complex database management, and more.

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

I.T., cybersecurity, and compliance are far too complex for one person to know it all. Like doctors, I.T. teams need specialists. An oncologist can't also be a dentist, ob-gyn, dermatologist, and general practitioner. And if you're making the mistake of putting ALL your I.T. into the hands of one person or a few people, you are making this mistake as well.

Suppose you only have a few people in your I.T. department. In that case, you might NOT be as prepared and capable as you may think to handle the rising complexity of I.T. systems for your growing company, the need to meet strict and growing compliance regulations, AND the overwhelming sophistication of cyber threats with the current resources, time and skill sets your I.T. team has.

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, and hardworking.

The fact is, NOBODY likes to go to the business owner 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 embarrassing for them to admit they don't have it all covered or lag 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 I.T. Leader 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, staff, and 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 five early warning signs that you may be pushing your I.T. department too hard:

1. **They're routinely working nights and weekends.** Everyone pulls an extended shift occasionally when a deadline is looming or due to a seasonal surge. But if your I.T. 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 significant projects?* It's common for I.T.

staff to be stressed to the max without the business owner/CEO/CFO knowing about it. **This will end up hurting your organization.**

2. **Projects aren't getting done on time or correctly.** Most business owners aren't technology experts, so it's difficult to know for certain if a project is taking longer than it should and 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. 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 I.T. leader rolled out any type of end-user security awareness training? Do they enforce strong passwords and compel employees to change their passwords routinely? Have they put together an Acceptable Use document or training to ensure employees know what is and isn't allowed with company e-mail, 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 I.T. 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.

5. **They aren't able to keep up with the latest technology trends** – Does your I.T. Leader have time to research the impact of Artificial Intelligence (AI) on your industry? Have they proposed ways to *safely* use AI to improve employee productivity or introduce training, policies, and controls to stop your staff from uploading sensitive corporate documents into an Artificial Intelligence engine designed to consume and then regurgitate information?

This May Be One Of The Biggest Dangers You Face

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

As I stated above, preventative maintenance is the FIRST thing that gets left undone when projects loom, and there are multiple fires to put out. Suppose your employees run into your I.T. team's office every five minutes needing a password reset or help to get their e-mail. In that case, it's hard to tell that employee "No" because the I.T. team is working on server maintenance or updating critical documentation.

The classic "important, not urgent" work 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, this is not an area you cannot ignore or cut corners.

When companies were fined or sued for a data breach, their WILLFUL NEGLIGENCE landed them in hot water. They knowingly refused or failed to invest in the necessary I.T. protections, support, protocols, and expertise 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 with "It won't happen to us." And you certainly don't want to underestimate the level of expertise you need.

These problems are unfortunately set to get worse. Hackers have already begun to use Artificial Intelligence to improve their phishing emails and identify weaknesses in your network. Cybersecurity experts are warning businesses that this next wave of AI-Enhanced Cyber-Attacks is on the horizon.

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 I.T. department is probably doing everything it can to protect you – **but it's up to YOU to be certain**. Everyone in your company – including your clients – depends 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 for 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, and Lawsuits:** Breach notification statutes remain one of the most active areas of the law. Several senators are lobbying for "massive and mandatory" fines and more aggressive legislation pertaining to data breaches and privacy. The courts are NOT in your favor if you expose client data to cybercriminals.

   Don't think for a minute that this only applies to big corporations: ANY business that

collects customer information must tell its customers if they experience a breach. Forty-seven states have data breach laws, including Texas – and they 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 healthcare business experiences a breach involving more than 500 customers, **it must notify a prominent media outlet about the incident. In addition, the company's name and the number of breached records are posted to a Federal Government website (known to some as the 'Wall of Shame')**. The SEC, FINRA, and many state regulating bodies also require financial services businesses to share details of any breach.

3. **Cost, After Cost, After Cost:** ONE breach, one ransomware attack, and one rogue employee can create HOURS of extra work for staff who are already maxed out when things are going well. Then there's a 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* 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 is the cost of legal counsel to help you respond to your clients and the media. Cash flow will be significantly disrupted, and budgets will be 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 data breach cost 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 understand the costs to your organization. (NOTE: Healthcare data breach costs are the highest among all sectors.)

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

   Harnish had $400,000 taken from his bank account when hackers were able to access his PC and intercept e-mails between him and his assistant. The hackers believed to be based in China, sent an e-mail to his assistant asking her to wire funds to three different locations. It didn't seem strange to the assistant because Harnish was then funding several real estate and investment ventures. The assistant responded in the affirmative, and the hackers, posing as Harnish, assured her it would 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 think that your staff is incapable of making a single mistake? A poor

judgment? **You don't believe you will be in a car wreck when you 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 not to 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 beliefs or political ideals.

   Even worse, they can take your client list and use it to send phishing e-mails and malware to your clients FROM YOU. I'm sure you would agree this would be totally and completely unacceptable – an embarrassing and gut-wrenching event you would NEVER want to deal with.

   Do you think this could *never* 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 damage or completely taken off guard?

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

GROWTH companies face the dilemma of needing professional-grade I.T. support but can't reasonably afford to invest in all the tools, software, and staff that it requires, which is precisely why we created a NEW solution we call Co-Managed I.T.

In short, Co-Managed I.T. is a way for business owners of growing companies to get the helping hands, specialized expertise, and I.T. management and automation tools they need WITHOUT the cost and difficulty of finding, managing, and retaining a large I.T. staff OR investing in expensive software tools.

This is NOT about taking over your I.T. Leader's 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" and then leave your team behind to try to support it (or give you the option of paying them big bucks afterward to keep it working).

It's also **NOT** just monitoring your network for alarms and problems, leaving your I.T. department to scramble and fix them.

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

Here are just a few of the reasons why business owners of similar-sized companies are moving to a Co-Managed approach:

- **We don't replace your I.T. staff; we make them BETTER.** By filling in the gaps, 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 headcount.** Let's face it: overhead walks on two legs. Plus, finding, hiring, and retaining TOP talent is brutally difficult. With Co-Managed I.T., you don't have the cost, overhead, or risk of a big I.T. team and department. We don't take vacations or sick leave. You won't lose us to maternity leave or an illness because we have to relocate with our spouse or we've found a better job.

- **Your I.T. team gets instant access to the *same* powerful I.T. 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 I.T. 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 I.T. program.

- **"9-1-1" on-site**. In the unexpected event, your I.T. 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 I.T. 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 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. CRITICAL MAINTENANCE WILL BE DONE.

- **We provide your I.T. leader and team with free workshops and training.** We offer regular workshops and webinars for our Co-Managed IT clients so they're more informed on critical topics such as cybersecurity, disaster recovery, compliance regulations, best practices, and more.

Scenarios Where Co-Managed IT Just Makes Sense

Scenario 1: Your in-house I.T. 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, maintenance, etc.

Scenario 2: Your in-house I.T. person is excellent at the helpdesk and end-user support but lacks expertise in advanced cybersecurity protection, server maintenance, cloud technologies, compliance regulations, etc. As in Scenario 1, we let them handle what they do best, and we fill in the areas where they need assistance.

Scenario 3: Your company is rapidly expanding and needs to quickly scale up I.T. staff and resources. 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: You have an excellent I.T. 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 business owner, the workload they are processing and how efficient they are (we call it utilization).

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.

Who This Is NOT For:

Although Co-Managed I.T. has many benefits, it is certainly not a good fit for everyone. Here's a short list of people and companies this won't work for.

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

  As I've said, 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 IT only works when both sides have mutual trust and respect.

- **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 I.T. leader's preferences, and we certainly will be flexible – to make this work, we HAVE to be.

  However, a big value we bring to the table is our 12 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, this only works if it's a collaborative relationship. But we cannot – will not – take on a client 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 I.T.**
  As a business owner, I completely understand the need to watch costs. However, starving an I.T. department of much-needed resources and support is careless and risky. Further, some business owners 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 one person – they are getting an entire team, a backup plan, tools and software, monitoring, and specialized skills.

  We can only help companies willing to invest sufficiently in I.T. – not elaborately or indulgently. We can demonstrate how a Co-Managed I.T. option is a far cheaper than building the same team independently.

A Full IT Department At A Fraction Of The Cost

To understand how Co-Managed I.T. saves you money and is a FAR superior choice to building your own I.T. department, you need to understand the structure and skill sets you'll require as a growing organization.

In most cases, you won't need these individuals' expertise 24/7/365 (like the CISO), but you WILL need that expertise, which is why outsourcing is the best strategy for a small or midsize business, especially now that I.T. talent is so difficult to find and expensive to hire.

Title	Purpose	Employees	*Salary
Help Desk Technician (Levels 1-3)	Responsible for being the first line of defense to troubleshoot end-users' problems, questions, and needs. Must be highly responsive.	1 per 70 employees	$35,000 – $50,000
Network Administrator	Responsible for maintaining your company's computer network (designed by the network engineer), ensuring it's up-to-date, secure, and operating as intended.	1 per 200 employees	$55,000 – $90,000
Network/Systems Engineer	Responsible for the strategic planning and implementation of the communication networks in your company.	1 per 200 employees	$63,000 – $100,000
IT Manager	Responsible for managing the helpdesk, network administrator, and systems engineer.	1 per 500 employees	$90,000 – $150,000

CIO (Chief Information Officer), CTO	Most senior technology executives inside an organization. Responsible for setting and leading the IT strategy for the entire company to ensure IT facilitates the organization's goals.	1	$100,000 – $150,000
CISO (Chief Information Security Officer)	Responsible for being head of IT security; creating, implementing, and managing a company's IT security policies to prevent a breach; meeting compliance requirements and insurance security standards.	1	$185,000 – $250,000
Total			**$438,000 – $640,000**

Additional IT Tools You'll Need:

- Helpdesk ticket management system
- Remote computer management and monitoring
- Technology documentation platform
- Asset management

What To Look For In A Co-Managed I.T. Partner

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

Here's why these options are not smart and won't deliver the value for your money.

For starters, if you have a productive, reliable I.T. leader or department, you want to keep those people on staff but make them more effective. No managed services provider can fully replicate the value that a full-time IT lead on your team 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.

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 will get better results if those projects are not a "one-and-done" where your hired I.T. company drops the solution in and takes off, leaving your I.T. 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.

Why We're Uniquely Positioned To Deliver Co-Managed I.T.

Our company is uniquely positioned to be your co-managed IT partner for several reasons, starting with the simple fact that we offer a customized bundle of IT services designed to support you and your team so you can bring more value to your firm.

Other IT companies provide short-term project-based services or only sell *Managed* IT services designed to replace you and your IT department. Others will offer simple monitoring but only that. True co-managed IT is NONE of those things.

We are a partner you can TRUST. We're the team that will sit up with you in the wee hours of the night to fix a problem. We're the team you can call when you're stuck or need an answer to a problem you've never seen before. We're YOUR team, YOUR champion.

We are an industry leader in this new model of Co-Managed IT. Having run a technology business for over twelve years, I know firsthand the challenges IT Leaders face when asked to protect a vulnerable asset against a growing threat and do it with a limited budget. To help, my colleagues and I wrote a best-selling book on how to protect your business from cybercriminals. I was also recently invited to speak on a panel with the FBI and Homeland Security to share with business leaders how they should prepare for and respond to a cyber-attack.

I have invested thousands of dollars and over a decade of my life 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 IT support you are giving your organization.

What Do Other Business Leaders In Texas Say?

"USM Technology is one of our most valued business partners! From day one, the USM team has been incredibly responsive, extremely patient, knowledgeable, and wonderful people to work with. They are truly exceptional!"

Rebecca Gibbs
Vice President
PEREGRINE INVESTMENTS

"USM has helped our company solve our most pressing challenges.

They did an exceptional job of helping us dial in the scope of our project and lay out a realistic project plan. Their smart team and diligence to a project plan have helped us automate 40 man-hours per month via Power BI reports & dashboards."

Matt Mettry
Chief Operating Officer
Gastroenterology of the Rockies

"They listened to us and designed a solution for our needs and budget. You won't regret your decision to choose USM! Now our traveling staff can securely communicate with clients, keep each other up to date, and share documents from their PC, tablet, or phone."

Rhonda Hunsucker NP
Founder and CEO
Collaborative Geriatrics Inc.

Think Co-Managed I.T. 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 or 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 particular needs, budget, and goals.

We work with your I.T. lead to determine areas that are lacking and to unearth potential problems such as 1) inadequate or outdated cybersecurity 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 I.T. systems and assets.

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

We can also answer questions you might have, such as:

- **Do I have sufficient redundancy and documented systems and processes in my I.T. department to avoid a single point of failure?**
- **Am I overspending and not getting my money's worth in any aspect of I.T.?**
- **Am I TRULY prepared and protected against ransomware attacks or cybersecurity breaches? Could I recover quickly? Am I meeting compliance regulations?**

The above is NOT designed to make your I.T. team look bad; as we all know, fresh eyes see new things. Your team is also 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.usmtechnology.com/consult.
2. Call us direct at 214-390-9252.
3. E-mail your appointment request to solutions@usmtechnology.com.

One Important Request

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

Even if you prefer that we work with your I.T. leader direct, I also urge you to be involved. I realize that I.T. may not be an area you 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 primarily with your I.T. lead but would request that 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,

Stephen Cracknell
CEO & Co-Founder
USM Technology

PS – If you would like to speak with any of our business owner/CEO clients utilizing our Co-Managed I.T. services, please e-mail me at stephen.cracknell@usmtechnology.com or call me at 214-390-9252 and I'll arrange for you to speak with them directly.