Special I.T. Leader 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: USM Technology
Author: Stephen Cracknell
202 South Austin Drive Allen, TX 75013

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

USM Technology

A Personal Letter from One I.T. Pro to Another

From the Desk of Stephen Cracknell
CEO & Co-Founder, USM Technology

Dear IT Leader,

I am Stephen Cracknell, the founder of USM Technology, a company that specializes in providing I.T. support and services to businesses throughout Texas. Before establishing USM 13 years ago, I worked at Microsoft for over a decade. During my tenure at Microsoft, I had the opportunity to help the *American Red Cross* enhance its disaster response capabilities. In the aftermath of Hurricane Katrina, the American Red Cross struggled to register the 10s of thousands of victims who required shelter due to the unprecedented flooding in New Orleans. My team and I automated and simplified registering victims in the Red Cross shelters. Our efforts were acknowledged by Bill Gates, who honored my team and me by personally giving us an award for our work at Microsoft's annual meeting. Since that career-defining moment, I have been committed to helping business leaders use technology to streamline their operations and prepare for disasters.

Because I understand the unique challenges mid-market I.T. leaders face, my team and I developed a unique service called Co-Managed I.T. designed to allow you to shine. This report will discuss what it is and how it can help you.

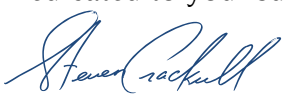
After all, we both know that in MOST organizations, I.T. is the most underappreciated and misunderstood function. Think about it: when was the last time you saw an I.T. person get "employee of the month" or make the cover of a magazine? The CEOs and C-suite of companies get interviewed and talked about on podcasts and TV shows. The sales team is showered with spiffs and bonuses, and freebies. The marketing team gets BIG prizes, recognition awards for a winning campaign, and 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 IT.

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 much time and money in 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 currently face.

Dedicated to your success,



Stephen Cracknell
CEO & Co-Founder
USM Technology

A Growing Crisis for I.T. Leaders

You are charged and held responsible for ensuring your I.T. systems are always up and 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, 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 need help 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 that 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, reputation, and possibly even your career are in peril when such an event happens.

So, what do you do about all of this?

One option is to ignore it. Keep to 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 will be okay. Assume you have it "handled." But you must 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.

One I.T. leader we work with had recently started in his position; the previous Director of IT had left him with ineffective and untested backups. A few weeks after he started, the organization was hit with a nasty strain of Ransomware. He spent six long weeks recovering their entire server infrastructure. Was it his fault? You can debate when a former employee's mistake becomes yours. But no matter whose fault, our client and his team experienced six painful weeks of stress, late nights, and forfeited weekends.

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 remotely in this "everything connected" world with multiple devices, multiple users who could 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," and every application connected to your network. Because of the cost, you can't possibly begin to have all the expertise you need under one roof. 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 a 20/20 vision of everything that is going on, but since 2010, 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.

The 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 cyber threats 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 intelligent, dedicated, capable, and 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 and sophistication of cyber-attacks and the damage they do.

3) Growing compliance regulations, making the cost of a breach or cyber-incident go up exponentially, with fines and penalties, not to mention the denial of insurance policies and the loss of clients who WON'T do business with your organization unless you have proper data protection and cybersecurity policies in place.

We've already seen multiple companies get slammed with sizable fines and settlements for security incidents due to lax security protocols, mistakes, and cover-ups. Do you really want this to happen to YOUR company on YOUR watch? One person simply can't know it all or handle it all.

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.

Preventative maintenance is one of the FIRST things that get left undone when urgent end-user problems pile up. Suppose your employees run into your office and/or your I.T. team's office every 5 minutes needing a password reset or help to get e-mail. In that case, it's hard to tell that employee "no" because they're working on server maintenance, reviewing security alerts, and patching PCs to protect your network.

The classic "important, not urgent" work 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 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.

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 as "It won't happen to us." And you certainly don't want to underestimate the level of expertise you need.

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

I'm sure you're doing everything you know to do to protect your organization – <u>but is it enough</u>? The sooner you can bring us in as your ally to focus exclusively on these matters and ensure no oversights, mistakes, or 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:**
   Do you think your [clients/patients] will rally around you when a breach happens? 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 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, 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. Multiple states are putting in place data breach notification and privacy laws that REQUIRE even small companies (and certainly larger organizations) to increase their steps to protect the 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 <u>that collects customer information also has essential obligations to its customers to tell them if they experience a breach</u>. Forty-seven states, including Texas, have data breach laws– and they are getting tougher by the minute.

   Suppose you're in health care or financial services. In that case, 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.

California's new CCPA law (California Consumer Protection Act) does not require that your business resides in California but simply that you have clients. More states are following these same paths of increased responsibility for companies, 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, 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 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, 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 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 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 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 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 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 overlooked 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 your staff cannot make 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 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 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 afterward to keep it working).

It's also **NOT** just monitoring your network for alarms and problems, leaving 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.** 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 don't have time to do, don't want to, or 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 wanted to get to but couldn't – or 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 you and your 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. 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 ready to assist with special projects, migrations, and new technologies – or to give you the ability to take some time off. We are <u>your</u> backup I.T. team!

Who This Is NOT For:

Although Co-Managed I.T. has many benefits, 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 view 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 mutual trust and respect exist 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 12+ years of expertise in supporting and securing computer networks. Therefore, the clients we get the best results for keep an open mind to 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.

- **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 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 far cheaper than building the same team independently.

Scenarios Where Co-Managed I.T. 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 essential 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, efficient, and competitive.

Scenario 2: You or your I.T. team are excellent at the helpdesk and end-user support but need more 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 rapidly expands 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: 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, manage, 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 genuinely know how much you handle daily? 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, 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 a full-time I.T. leader's value. They will try to sell the CEO and CFO on that idea, promising incredible cost savings. Still, 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 be higher because they need to make a 60% to 70% margin on services. **Outsourcing only makes sense when a FULL-TIME person is not required or when** very specialized skills are needed that are difficult to find and (again) not required full-time.

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 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 will 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 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 provide will dramatically improve your effectiveness and the quality of IT support you are giving your organization.

What Do Other I.T. Leaders In Texas Say?

We have worked with USM for years on various Microsoft implementations, from reporting to infrastructure to security. USM's team has proven competent and capable across all our engagements.

Their executives also proactively update us on Microsoft's newest technologies and help us align them with our organization's business priorities.

The best part about working with USM is that we now have a ***Trusted Advisor*** when implementing Microsoft's Cloud Services.

~Craig
Vice President of Information Technology
Financial Industry

"We were searching for a group to help us fortify our cybersecurity posture. USM came in with compelling recommendations and the skills and talent to help us rapidly implement those enhancements. I sleep better at night knowing that USM's cybersecurity systems are at work protecting our network.

USM has gone on to help us streamline our operations, licensing, and employee productivity. We simply no longer need multiple consulting firms to get things done. Their responsiveness is far better than any technology firm we have worked with.

USM Technology is an **excellent choice for over-worked IT people**!"

~David
Director of IT
Construction Company

"USM has a team of dependable US-based technology professionals that respond quickly to our requests for assistance. They routinely help us optimize our Microsoft 365 environment and work closely with us to secure our network.

USM is an **integral part of our technology department**."

~ Shawn
I.T. Manager & HIPAA Security Officer
Hospital System

My technology team and I worked closely with USM to design and deploy our Microsoft 365 platform, eliminating multiple legacy technologies. Our staff seamlessly collaborates across the organization, sharing documents, coordinating projects, and securely communicating with our clients.

The team at USM handled the backend data transfers and permissions and provided exceptional training and support to our employees, ensuring a streamlined transition to Microsoft 365. Their support allowed **my team and I to focus on our strategic initiatives**.

~Aaron
Information Systems Manager
Home Health Network

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

Suppose this letter has struck a chord, and you want to explore how a Co-Managed I.T. relationship would benefit you and your I.T. department. In that case, we've reserved initial telephone appointment times with our senior consultants to evaluate your situation and

recommend the Co-Managed I.T. approach that would work best based on your 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 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 in 3 ways:

1. Go online to: www.usmtechnology.com/consult
2. Call us direct at 214-390-9252.
3. E-mail your appointment request to…my assistant at hello@usmtechnology.com.

One Important Request

We strongly encourage you to bring your CEO/CFO into this Diagnostic Consultation earlier rather than later, especially if they need to be brought "on board" with this concept. In most cases, they are giving 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 entirely agrees that you are understaffed and overwhelmed and need 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.

Stephen Cracknell
CEO & Co-Founder
USM Technology

P.S. If you would like to speak with any of the I.T. leaders 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.