About the Author

For over 15 years, Jason Kirkhart has been a noteworthy leader in providing managed IT services to small businesses in Southern Virginia and North Carolina. As founder and CEO of Beetoobi IT Solutions, a full-service tech firm specializing in health care IT, Jason is driven by his passion for improving the health of a community by protecting its medical networks – a task that cybercriminals and extreme medical industry regulations don't make easy.

Married to a pediatric nurse practitioner for two decades, Jason has a front-row seat in the complicated world of medical practices. They must deal with comprehensive protocols, chronic understaffing, and worldwide health care crises – all without the resources that larger medical institutions have. Hackers see this too and often target small practices, seeking to pry open their vulnerabilities through vicious online attacks like ransomware. But Jason knows that medical practitioners need to focus on enhancing the quality of life of their patients, not preventing greedy hackers from probing their network and stealing highly confidential information. That's why he takes pride in providing the best cyber security and regulatory services possible to small and medium medical practices. This allows health care providers to do what they do best and provide exceptional health care to their communities.

Under Jason's leadership, Beetoobi has been honored with a local award for Best IT Consultant, recognizing his extraordinary commitment to creating safer and more secure health care IT infrastructures. Jason and his wife, Senecca, are parents to two teenage sons, and when he's not busy at home or work, he can be found coaching the local high school volleyball teams or playing a round on the golf course. Jason and his family currently reside in Southern Virginia.

The C-Suite's Dilemma

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

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

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

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

Further, if your organization is NOT properly invested in cyber-protection and backup technologies, one cyber-attack or data-erasing event could have serious, long-lasting, costly ramifications – or even put you out of business.

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

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

Your "Category 5" might be a ransomware attack or data breach where clients and employees' personal data is compromised. It very well could be a disgruntled, rogue employee that decides to take revenge by erasing data or selling and posting it online. It might be a failed server that went down, taking all its data with it, never to be revived again. It might be a corrupt SQL database that is beyond their expertise to fix.

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

But if you are like most of the CEOs, we work with to deliver co-managed IT, your IT person or department is significantly understaffed, overwhelmed and simply not able to keep up with the growing demands your company is putting on them. They also may be

lacking in specialized knowledge about any number of things – data backup and disaster recovery, cyber security protections, secure cloud computing, complex database management and more.

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

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

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

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

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

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

Signs You Are Pushing Your IT 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, more staff, more help. They are trying to be good stewards of your company and budget – so it's up to YOU as the leader of your organization to ensure you are not setting them up for failure or burnout.

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

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

It can also lead to important details being skipped and mistakes being made.

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

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

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

4. **They aren't rolling out PREVENTATIVE security measures.** Has your IT leader rolled out any type of end-user security awareness training? Do they enforce the use of strong passwords and compel employees to change their passwords routinely? Have they put together an Acceptable Use document or training to make sure 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 IT person or department is overwhelmed – but these are critical for insurance purposes and reducing the chances of a cyber-attack or other disaster that would carry significant financial losses and/or hurt your company's reputation.

More CEOs Are Getting Fired Over Cyber Security Incidents Than the CIOs Or Information Security Officers They Employ

Without a doubt, the one area that you are most at risk for with an incomplete, inefficient, and understaffed IT department is a lack of proper cyber security protections. One incident can lead to data loss, extended downtime and (potential) liability with a cyber security breach or compliance violation – all expensive risks that CAN be prevented.

According to a report by Gartner titled, "8 Reasons More CEOs Will Be Fired Over Cybersecurity Incidents," twice as many CEOs are getting fired over cyber security incidents than the CIOs or CISO (Chief Information Security Officer) they employ.

This is because:

- CEOs and other non-IT executives treat cyber security like the "dark arts," and therefore do not properly address or fund cyber security issues.

- CEOs continue to treat cyber security as a *technical* problem and bury in the IT department instead of making it part of all key business decisions.

- Most CEOs believe they have a "good" security program – but don't really know if they are taking the right steps and have zero verification systems in place.

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

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

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

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

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

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

Yes, your IT department is probably doing everything they can to protect you – **but it's up to YOU to be certain**. Everyone in your company – including your clients – 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/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 outlined in this report or will you have to tell your clients, "Sorry, we got hacked because we didn't think it would happen to us," or "We didn't want to spend the money." Is *that* going to be sufficient to pacify those damaged by the breach?

2. **Government Fines, Legal Fees, Lawsuits:**
   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. The courts are NOT in your favor if you expose client data to cybercriminals.

   Don't think for a minute this only applies 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 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 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.

3. **Cost, After Cost, After Cost:** ONE breach, one ransomware attack, one rogue employee can create HOURS of extra work for staff who are already maxed out when things are going well. Then there's business interruption and downtime, backlogged work delivery for your current clients. Loss of sales. Forensics costs to determine what kind of hack attack occurred, what part of the network is/was affected and what data was compromised. Emergency IT restoration costs for getting you back up if that's even possible. In some cases, you'll be forced to pay the ransom and maybe – *just maybe* – they'll give you your data back. Then there are legal fees and the cost of legal counsel to help you respond to your clients and the media. Cash

flow will be significantly disrupted, budgets blown up. 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 IT recovery costs, lost revenue, downtime, fines, legal fees, etc.** How many client records do you have? Employees? Multiply that by $225 and you'll start to get a sense of the costs to your organization. (NOTE: Health care data breach costs are the highest among all sectors.)

4. **Bank Fraud:** If your bank account is accessed and funds are stolen, the bank is NOT responsible for replacing those funds. Take the true story of Verne Harnish, CEO of 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 that your staff is incapable of making a single mistake? A poor judgment? **Nobody believes they will be in a car wreck when they leave the house every day, but you still put the seat belt on.** You don't expect a life-threatening crash, but that's not a reason to not buckle up. *What if?*

5. **Using YOU as The Means to Infect Your Clients:**
   Some hackers don't lock your data for ransom or steal money. Often, they use your server, website, or profile to spread viruses and/or compromise other PCs. If they hack your website, they can use it to relay spam, run malware, build SEO pages, or promote their religious or political ideals.

   Even worse, they can take your client list and use it to send phishing e-mails and malware to them 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 have to deal with.

6. 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 IT team be brilliantly prepared to minimize the damage or completely taken off guard?

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

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

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

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

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

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

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

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

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

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

spouse, or we've found a better job.

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

- **"9-1-1" on-site**. In the unexpected event your IT leader was unable to perform their job OR if a disaster were to strike, we could instantly provide support to prevent the wheels from falling off by instantly stepping in. And because we'll already have knowledge of your business, your systems, and data, we can transition quickly in without downtime.

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

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

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

To Schedule Your FREE Consultation,
Please visit www.beetoobi.com or call our office at 434-446-1035

Scenarios Where Co-Managed IT Just Makes Sense

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

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

Scenario 3: A company is in rapid expansion and needs to scale up IT staff and resources quickly. This is another situation where our flexible support services can be brought in to get you through this phase as you work to build your internal IT department. Hiring IT talent IS difficult and expensive, and your HR resources can be better served in other areas.

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

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

A Fully Competent IT Department, Cyber Risks Mitigated And A 19% To 41% Cost Savings

On average, we save our clients between 19% and 41% on total IT department costs. This cost reduction is mostly secured in the lowered cost of finding, hiring, managing, and retaining all the skills you'll need for competent IT department, as well as in providing "fractional ownership" of the proper tools, software, and operational systems you need for them to be efficient.

On the next page is a list of the hands-on support and SKILL SETS you will need to have at your disposal. You might not need these individuals' expertise 24/7/365 (like the CISO), but you WILL need that expertise at some level guiding and managing your IT.

Title	Purpose	Staffing	*Salary
Help Desk Technician (Levels 1-3)	Responsible for being the first line of defense to troubleshoot end-users' problems, questions and needs. Needs to 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 help desk, network administrator and systems engineer.	1 per 500 employees	$90,000 - $150,000
CIO (Chief Information Officer), CTO	Most senior technology executive inside an organization. Responsible for setting and leading the IT strategy for the entire company to ensure IT facilitates the goals of the organization.	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.	1	$185,000 - $250,000
Total			$438,000 - $640,000

Additional Management Tools Your IT Department Should Have, But Doesn't:

Keep in mind that these tools are to manage your network, users, data, and security. These are *in addition* to the usual software and security applications (antivirus, spam filtering, backup systems, etc.) and are designed to allow your IT team to do their job with maximum efficiency and effectiveness, delivering the best IT experience for you and your employees.

Most small to mid-sized IT departments will NOT have these tools in place due to the cost of buying them and the complexity of setting them up. As a Co-Managed IT client, we set up and provide your IT department with these tools as part of the service, fully customized to your environment, without the heavy cost of owning them outright.

Further, these tools allow us to step in at a moment's notice to assist in situations where additional help is needed (overflow), when your IT team needs assistance in resolving a critical problem, or in the event one or more of your IT team quits or is unable to work for any unforeseen reason.

- **Helpdesk Ticket Management**: This is a core component of your IT department, allowing us and/or your team to capture, prioritize and respond to your employees' requests for IT services so problems get resolved quicker and far more efficiently.

- **Remote Monitoring and Management Software:** Computer networks need constant monitoring for problems. Having this tool allows us and/or your IT department to be notified of a problem so it can be resolved quickly, similar to how newer cars alert you to low tire pressure, low oil, or other engine problems. This software also enables your techs to remotely access devices and PCs to resolve problems, which is essential if you have a remote or mobile workforce.

- **Network Documentation:** Without good network documentation, diagnosing and resolving problems takes longer, which means more downtime and more costs. Further, if an IT person leaves an organization, without proper documentation of the network, ALL their knowledge about the network, history of problems, software licenses, hardware, and devices leave with them, making it infinitely more difficult and time consuming for another IT person to take over.

Who Co-Managed IT Is NOT For:

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

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

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

- **IT leaders who don't have an open mind to a new way of doing things.**

  Our first and foremost goal is to support YOU and your IT leader's preferences, and we certainly will be flexible – we MUST in order to make this work.

  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 before, this only works if it's a collaborative relationship. But we cannot – will not – take on a client that is doing things we feel compromise the integrity and security of a network, even if that's "how we've always done things" or because "that's what we like."

- **Organizations where the leadership is unwilling to invest in IT or be serious about cyber security and complying with data protection laws.**

  As a CEO myself, I completely understand the need to watch costs. However, starving the IT department of much-needed resources and support is risky and provides false savings. 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 that one person cannot fulfil.

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

What to Look for In A Co-Managed IT Partner

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

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

For starters, if you have a productive, reliable IT leader or department, you want to keep those people on staff, but make them more productive. No managed services provider can fully replicate the value that a full-time IT lead on your staff can deliver. They will try to sell you on that idea, but candidly, they won't be able to allocate the time and attention that a full-time employee can.

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

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

A better approach is a co-managed IT environment when a solution is implemented by the same team that is supporting it.

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

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

We are also the leader in efficient, responsive IT services and support. What makes us unique is that our business is designed with YOU in mind. We value your time and your input. We'll listen to what you say, offer our advice, and draft a plan together. We have a solid reputation for service built on over 12 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, ransomware, cloud technologies, etc.

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

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

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

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

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

We can also answer questions you might have such as:

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

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

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

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

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

To Schedule Your FREE Consultation,
Please visit www.beetoobi.com or call our office at 434-446-1035

One Important Request

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

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

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

We look forward to working with you and your team.

BEETOOBI

IT SOLUTIONS

3318 Old Halifax Rd, South Boston, VA 24592 | 434-446-1035 | www.beetoobi.com