Special C-suite Report

# The Executive's Guide To Co-Sourced IT

A far superior approach to lowering the risk, difficulty, and cost of addressing cybersecurity, compliance, and IT support for your growing organization

Provided By: **Affiliated Resource Group**
Author: Michael Moran

5700 Perimeter Drive Suite H
Dublin, Ohio 43017
**www.aresgrp.com - 614-495-9658**

AFFILIATED
Cybersecurity, Compliance, & Managed IT Support

# Introduction

It's no secret: Due the economic crisis we've all been plunged into, executives and IT leaders are under enormous pressure to cut operational costs while finding creative ways to continue to transact and fulfill on contracts and services.

Now more than ever, it's ESSENTIAL that your IT functions not only perform, but keep you secure from cyber-attacks, data loss, and potential compliance violations with employees working in the office and from home in unsecured, unmonitored environments.

Outsourced IT support and internal IT teams both have their pros and cons, but there is a third option available to businesses – a Co-Sourced IT relationship. Co-sourcing is a flexible approach which allows you to supplement your internal IT team with an external solution that can provide the focused, experienced resources, tools, and processes that can alleviate the internal team's workload, improve IT functions and maturity, and address your cybersecurity and compliance needs in a reasonable, cost effective manner.

I'm confident this white paper will help you better understand the significance of these issues and the options that are available to your organization.

If you have any questions or would like to discuss your options in detail, please reach out to me at **614.495.9658** or email me at **michaelmoran@aresgrp.com**. I'll be happy to help you explore if Co-Sourcing with your IT team is a good fit for your organization.

**Mike Moran**
President
Affiliated Resource Group
Columbus, Ohio

# Table of Contents

# 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, executives 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, cybersecurity risks, 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 cybersecurity and disaster recovery protections.

However, no company can afford to lag behind in IT investments. 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.

It can easily be argued that Technology is the one resource (besides cash), that if used effectively, can help successfully scale an organization faster, more efficiently, and more cost effectively than any other resource.

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?**

1. 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.
2. Trust that your current IT department has it "handled."
3. Hire more people and buy more expensive "tools".
4. Outsource everything
5. Look for alternatives

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 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. There are plenty of foreseen and unforeseen scenarios that put your company in a catastrophic situation that could be hard to recover from.

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

But if you are like most of the executives we work with to deliver Co-Sourced IT, your IT team is understaffed, overwhelmed with all of the responsibility, 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, cybersecurity protections, compliance requirements, secure cloud computing, complex database management, and more.

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

Fact is, your IT team might NOT be as prepared and capable as you may think to handle the rising complexity of IT systems for your growing organization, 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 and disruption to your overall operations.**

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 boss 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 Your IT Team Is Stressed Out Or At Their Max

Conscientious IT leaders and staff often WON'T help you understand they need more resources or more help. They are trying to be good stewards of your organization 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 some warning signs you may be pushing your IT department beyond their capacity:

**1 . They're routinely working nights and weekends – and even on "vacation"**

Everyone pulls an extended shift once in a while when a deadline is looming or due to a seasonal surge. But if your IT team 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. Turnover risks also increase significantly. 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 management team even knowing about it. *This will end up hurting your organization.*

**2 . Projects aren't getting done on time or correctly**

Most business leaders 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 – and most IT resources are not experienced project managers. All too often, a business leader will jump to the conclusion that the IT team is incompetent or lazy – but that may not be the case at all. It could be they're so overwhelmed with other, "urgent" tasks and putting out fires that they can't GET the time to do the project properly. *This costs your organization productivity and possibly competitive advantage.*

**3 . Changes in Approach or Attitude**

Some employees will "suck it up" and push through, not wanting to talk to you about desperately needing more help. Or maybe they have tried to bring it up, only to be shut down due to a lack of effective communication and justification for the requests. 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. *This ineffective communication and lack of progress on risks and potential exposures can result in major loss and disruptions to your mission.*

**4 . They aren't addressing PREVENTATIVE security measures effectively**

Do you have a consistent, tracked, end-user security awareness training program? IS your password policy enforced? Is your Acceptable Use policy in place? How often do they regularly validate that the policies that need to be formalized are implemented and are being accomplished as expected? 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 reducing the chances of a cyber-attack or other disaster that would carry significant financial losses and/or hurt your reputation.*

## This May Be One Of The Biggest Risks You Face

Without a doubt, the one area that you are most at risk for with an overwhelmed and understaffed IT department is data loss, extended downtime and (potential) liability with a cyber security breach or compliance violation.

As stated above, the FIRST thing that gets left undone when 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 documentation.

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

To make matters worse, the complexity of knowing how to protect your organization against cybercrime and be following 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 can't any longer 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 – are depending on you.

# 5 Risks To Your Organization

Your IT team is challenged every day to support the application and systems needs of your organization. They have many responsibilities - in most cases they also have responsibility for your key application support; insuring your users and the organization effectively uses the application systems you've purchased to run the organization successfully and to prevent revenue leakage, wasted productivity, billing and reimbursement errors, and that the system is at a level required to maintain support from your vendors .

In addition, they have the responsibility to secure the organization from threats and cybersecurity risks - they may use products and third party services to assist with that effort; however, they have not set up or used the solutions they've chosen before, nor had the proper training and support they need to effectively utilize the tools in your environment – leaving you with an exposed environment.

That is a lot to shoulder on a small group of people – and leaves the organization with exposed risks – here are some of them that will occur when you are not adequately protected and an issue occurs.

### 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 in putting in place the protections needed 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 . 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 revenue. 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 disrupted, budgets blown up. Some states now mandate multiple forms of compensation 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.)

### 3 . 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 to the request email 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?

### 4 . 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. 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 damages or completely taken off guard?

### 5 . 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 healthcare 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).

# Co-Sourced IT: Solving The IT Maturity Dilemma

In short, Co-Sourced IT is a way for 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" (although in our case, we do help a majority of our clients with their projects).

It is a flexible partnership to help you get the right level and amount of additional IT support, tools, and services at a much lower cost. Here are just a few of the reasons why CFOs of similar-sized companies are moving to a co-sourced 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.

- **You don't have to add to your head count.** Let's face it: overhead walks on two legs. Plus, finding, hiring and retaining TOP talent is brutally difficult. With Co-Sourced IT, you don't have the cost, overhead or risk of a big IT team and department. We don't take vacations, sick leave, or relocate with our spouse because they found a better job.

- **Your IT team gets instant access to the same powerful IT automation and management tools we use to make them more efficient.** 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-Sourced IT program.

- **Your organization and IT team gets access to the cybersecurity and compliance processes we use to help our clients achieve their requirements and do it more efficiently.** Our approach will enable your team to protect against or resolve threats and issues faster, establish a communication process to manage risks and be more efficient. These are a suite of tools, processes, and policies, your company may not consider on your own, but they can be included with our Co-Sourced 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 and prevent additional lost productivity or other errors that can happen under stress.

- **You get a TEAM of smart, experienced IT pros.** No one IT person can know it all. Because you're a co-sourced 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 your 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.

- **We provide your IT leader and team free workshops and training.** We offer workshops and webinars for our Co-Sourced IT clients so they're more informed on critical topics such as cyber security, disaster recovery, compliance regulations, best practices and more.

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

# 5 Scenarios for A Co-Sourced IT Relationship

Over the past 10 plus years, we have worked with several dozen organizations to help provide a Co-Source solution to meet their ever changing it needs. The following examples represent five common scenarios that we have found to be the most advantageous in supporting a Co-Sourced environment to help you align your technology resources to achieve your goals faster.

**Scenario 1**

Your in-house IT staff is better served working on high-level strategic projects and initiatives, or supporting your applications, but needs support in getting day-to-day tasks completed, such as troubleshooting various problems that arise, addressing IT operations functions (patching, tools deployment and management, monitoring system alerts for issues/threats, etc.), providing help-desk resources to your employees, software upgrades, data backup and maintenance, etc.

**Scenario 2**

Your IT resource is responsible for everything IT and does not have a backup or "additional set of hands" to help with support, some technology issues, or strategy. All of the knowledge is "in their head" and taking time off really is not feasible as they are on call – even on vacation. You want to provide them with the opportunity to be balanced and to protect the organization, yet adding additional staff is not a reasonable option.

**Scenario 3**

You are in rapid expansion mode and need to scale up IT resources quickly to support the needs of the organization. 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 leadership team, the workload they are processing and how efficient they are (we call it utilization) as well as our processes for validation of the important IT operational function that leadership needs to have validated on a regular basis to meet organization and regulatory expectations.

**Scenario 5**

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

# An Operationally Mature IT Department, Cybersecurity, and Compliance Risks Successfully Mitigated

## *And A Potential 19% To 41% Cost Savings*

**On average, our Co-Sourced solutions save our clients between 19% and 41% on their true IT department costs.** This cost reduction is addressed in a number of areas, including eliminating the 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, operational systems, and processes you need for them to be efficient.

Below is a list of the hands-on support and SKILL SETS you will need to have at your disposal. You might not these individual's expertise 24/7/365 (like the Security Analyst), but you WILL need that expertise at some level guiding and working with your IT team. Let's break down these costs:

### 1. Technical Support (help desk resource)

Your first line of defense people must be highly responsive and resolve issues quickly and efficiently via telephone and email; handle issues with desktops, telephones, printers, and things like password resets.
Average Annual Cost: $45,000 - $70,000

### 2. Network Administrator

Resource responsible for making sure all servers, software, networked systems, and backup systems run smoothly and are properly maintained.
Average Annual Cost: $55,000 - $80,000

### 3. Network Engineer

This person must understand the company's overall business and technology strategy and be able to make important decisions around software, systems and processes. This resource is also involved with setting up cybersecurity tools and device configurations.
Average Annual Cost: $75,000 - $120,000

### 4. Systems/Applications Analyst

This resource understands the organizations applications and is a "super user" of the system or sections of the system and works with users to maximize productivity. Coordinates requirements for enhancements or additional needs, and helps with documentation of processes and procedures.
Average Annual Cost: $65,000- $120,000

### 5. Security Analyst/Architect

Resource responsible for establishing or managing the organization's security approach and processes. Requires both tools and processes to help reduce threats and exposures as defined by the organization's leadership Risk Management/Threat Tolerance plan.
Average Annual Cost: $75,000 - $150,000

### 6. Manager/Director of Technology

This role is an oversight role, that in addition to still having some technical/application management responsibilities, can coordinate, manage and improve an organization's technology environment and processes. They are responsible for resource and environment operations and management, IT strategy planning and budgeting.
Average Annual Cost: $100,00 - $150,000+

To properly provide the organization with the necessary technology staff to keep your systems running smoothly and safely, you could need to spend anywhere over $400,000 annually in payroll costs alone!

Considering an organization with 100 users may only need a number of these roles for only part of the time, a Co-Sourced solution that brings the skill sets when they are needed can you with a greater efficiency and benefits at a fraction of the cost.

**Additional Management Tools Your IT Department Should Have, But may not:**

Keep in mind that these tools are to manage your network, users, data and security. These are replacements and in addition to the usual security applications (antivirus, spam filtering, backup systems, etc.) and provided by resources focused on these functions as their job – not an additional task – and are designed to allow your IT team to focus on their defined tasks 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-Sourced IT client, we have the flexibility to provide a solution that meets your needs, 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 is on vacation, or is unable to work for any unforeseen reason.

**Tools**

- ADVANCED ENDPOINT DETECTION & RESPONSE Real-time protection with Advanced A.I.
- Comprehensive ANTI-VIRUS SOLUTION to protect your devices with real-time protection with Advanced A.I.
- 24/7/365 OPERATIONS CENTER staffed by experienced Engineers to identify and process alerts/issues
- NETWORK VULNERABILITY SCANNING (Standard)
- CONFIGURATION CHANGE MANAGEMENT Tracking – to track changes to system configurations
- SERVER & NETWORK MONITORING (Standard) Downtime and Performance Degradation Alerts & 24/7 notification
- REGULAR ENDPOINT PATCHING -- Device Security Patching & Compliance Reporting
- ONLINE TECHNICAL DOCUMENTATION SYSTEM - Maintain inventory and systems configurations, warranty/maintenance tracking
- END-USER SECUIRTY TRAINING & AWARENESS including Bi-Weekly Simulated Phishing with Micro-Learning training, full tracking and reporting
- MONITORING THE WEB FOR COMPROMISED CREDENTIALS to identify risks and

- FULL MANAGED BACK UP SOLUTION with incremental backups for 30 days on site and up to 365 days in an encrypted, off-site data center. Includes regular test restores and verifications

- TICKET MANAGEMENT SYSTEM: 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.

- ENVIRONMENT DOCUMENTATION: Without good network documentation– including licensing, configurations, policies information, 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 of their knowledge about the environment leaves with them, making it more difficult and time consuming for the next resource.

- IT ROADMAP: Tool used to help identify the IT strategy to keep it aligned with organization's goals; identifies steps and planned activities in IT (including budget).

These tools can cost between $20-$28.00 per user per month to own; then proper configuration and daily operating processes need to be created and followed to ensure they are being properly deployed and used in your organization.

For a 100 user organization, that means you would need to expend between $24,000 and $30,000 annually in tool costs to effectively support your organization.

**IF you need help with your IT operations and management needs, and are not in a position to be expending upwards of $400,000 annually on IT resources, you should consider Co-Sourcing.**

# Why Select Affiliated To Deliver Your Co-Sourced IT

There are a number of reasons our company is uniquely positioned to be your Co-Sourced IT partner, starting with the simple fact we're the one of the best IT firms in the Columbus area. And we have successfully doing IT Co-sourcing for over 15 years.

Other IT firms provide short-term project-based services, monitoring only or only sell managed services designed to replace your IT department. True Co-Sourced IT is NONE of these things.

Affiliated is 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 a recognized local leader in efficient, responsive IT services and support. We currently serve over 80 organizations in the central Ohio region and have a solid reputation for service built on over 25+ years of experience. But that's not all we do. We are also the leading/preeminent experts in cybersecurity solutions based on fundamental IT Operations execution – experienced in our thorough understanding of how to protect networks from data loss, ransomware, and cloud technologies.

We have invested hundreds of thousands of dollars and over 25+ years into developing the most efficient, robust and responsive IT support solutions so you don't have to. The co-sourced IT support we provide will dramatically improve your effectiveness of your IT team while saving you money.

1. **Our Focus Is On You**
   We focus on our client's success and that focus leads to long-term relationships. More than 80 percent of our clients have been working with us for over five years.

2. **We Specialize In Growing Companies**
   That means we understand your incredibly hectic and stressful work schedule and WHY it's critical to remove obstacles, frustrations and technical problems to keep you productive. We know the systems you work with and focus on making them work seamlessly to improve your efficiency by eliminating extra steps, minimizing workarounds, and reducing manual effort. We also have tech support available 24/7/365 since we know you don't work the normal "9-5" day, and can help you maintain the freedom to work remote while making sure you meet compliance standards for data security and backups.

3. **Industry Expertise**
   We've developed expertise in the Manufacturing, Distribution/Supply Chain, Professional Services, and Healthcare industries for organizations with 50 to 250+ users. We have over 25+ years' experience working with these clients and are familiar with what is important to you.

4. **Address Your IT Needs – From Vision Through Long-Term Support**
   Our solutions can assist from vision to design and planning, to product specification through pricing and acquisition, to installation, implementation, documentation and project management, to post-project support of you and or your users. This allows you to have one consistent team to work with and provides more efficient service and support for you and your team.

5 . **Flexible, Tailored-To-Your-Needs Support Options**

Affiliated provides Co-Sourced Solutions in a variety of options - for organizations that need a complete back end IT infrastructure services solution or companies that have IT staff and need additional help or specific functions to complement their team. Affiliated provides our customers with a variety of managed support options, ranging from back-end maintenance and monitoring for issues, to user help-desk support with ticketing, to strategy and budget and asset/license lifecycle management. We have successfully provided these services for over 15 years and can create a solution specifically for you and your team.

6 . **Policy and Procedures frameworks and assistance**

Policy reviews and actual template documents to help you implement the appropriate level of process to protect you, your organization, and your data.

7 . **Certified Experts On Staff**

Unlike other IT firms, who have one or two guys trying to juggle multiple projects and wear various hats, we have a team of vendor certified engineers on staff with diverse, specialized areas of expertise who work together to deliver the most effective and correct solutions to you. We assign the right team to fit your IT needs.

8 . **Leverage Our Vendor Relationships To YOUR Advantage**

Having an advanced level of partnership with key vendors (e.g. Microsoft, VMware, and Dell) allows us access to special support levels that most "partners" do not have. We are able to get additional vendor support and can provide the right assistance, validated by the vendor, so if any issues come up, we work lockstep with you to get them resolved quickly and effectively.

9 . **Support Both On-Premise And "Cloud" Solutions**

Some IT firms offer or recommend only one solution because otherwise THEY make less money. Our philosophy is – and always has been – to offer what's BEST for you. That's how we keep so many clients long-term. We'll base our recommendations on what YOU want and what YOU feel most comfortable with. Our job is to lay out your options, educate you on the pros and cons of each and guide you to the best, most cost-effective solution for you.

10 . **All Projects Are Completed As Agreed On and On Budget**

When you hire us to complete a project for you, we won't nickel-and-dime you with unforeseen or unexpected charges. We guarantee to deliver precisely what we promised to deliver, on time and on budget. We can offer our agreements on a fixed-fee basis so you know exactly what you're going to pay.

11 . **One Of A Few Elite Microsoft Office 365 Partners In The Country**

They call us their "SMB Champions" (SMB stands for small-medium business). Migrating (or setting up) Office 365 and other cloud solutions is NOT something you want to attempt on your own. There are dozens of ways an improper setup can cause problems, systems that don't work, lost data and e-mail, and a host of other problems – you need someone with experience in multiple environments with a variety of clients. We have that experience – from a small office with 30 employees to a full Office 365 migration for a customer with 1,000 employees; we can help.

# Executives and IT Leaders Share Their Experiences

## Affiliated's Value and Services have Exceeded our Expectations

For me, the single biggest benefit of working with Affiliated has been their ability to help with strategic planning for our expansion and growth. From setting the strategy with our IT team, to coordinating hardware and software purchases and infrastructure upgrades, to collaboration on projects and troubleshooting issues, covering our cybersecurity needs, they bring a high level of experience to every facet of our IT eco-system. And because the entire Affiliated team has taken the time to understand our business and needs, they have been critical to our success in aligning our IT department's goals to our overall company goals. It is a strong partnership and has been for over 10 years.

***– Craig Casdorph, CFO, Buckeye Power Sales***

## Affiliated Provides Experienced Strategic IT Planning for Expansion and Growth

The biggest benefit to Buckeye Shapeform has been the speed, professionalism and value of the services that the Affiliated team has provided. We need our systems up and available to keep us productive - we have to deliver to our customers on time. Our employees have found Affiliated's team easier to work with and more responsive than our previous providers. Knowing that when we contact them, we get a technical person on the phone to help immediately is a huge benefit and getting problems solved quickly is important and has dramatically reduced our down time. Our management team now spends its IT time deciding on recommended turnkey options, not trying to validate solutions - then managing getting them installed correctly. As the executive of the company, I get fewer issues on my desk, which allows me to focus on growing our business and supporting our customers.

***– Steve Parker. President/CFO, Buckeye Shapeform***

## A Responsive and Effective Team I can Count On

Under the Co-Sourced program, Affiliated has taken a lot of work off my plate so I can focus on bigger priorities. It has allowed me to be more proactive in managing the health of our IT infrastructure and provide support to our users much faster. Whether working with me on a big IT project, keeping us updated, or troubleshooting a potential cybersecurity issue, this program makes it much easier and more affordable for us to provide the IT systems and support our users need and expect to focus on their jobs.

***– Steven Schaar, Information Technology Director, Kenda Tire***

## Affiliated Secured Our IT Infrastructure and Improved Our HIPAA Compliance

The team at Affiliated has helped us to cost-effectively improve and secure our IT infrastructure to allow our team to implement a new EHR system to support our residents, secure, and expand our capabilities to multiple facilities without growing our IT team, and address our IT sections of HIPAA compliance and with their Risk Assessments and OCP (Ongoing Compliance Program) solutions. They are helping us stay secure and compliant. I had worked with them for almost 8 years in a prior organization and knew their abilities; they have really been a great partner – and I can rely on them whenever I or our organization needs assistance.

***– Penny Harris, IT Director, Mother Angeline McCrory Manor & Villas at St. Therese***

# Considering Co-Sourced IT?

## Our Cyber-readiness Review Will Help You Decide

If this Whitepaper struck a chord and you want to explore how (if?) a Co-Sourced IT relationship could benefit your organization, please call us to evaluate your specific situation and recommend the Co-Sourced approach that would work best based on your specific needs, budget and goals.

We will work with you and your IT team 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.

The review is designed to help you and your IT team identify areas that can be improved to help you and your team be more effective. 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.

**The next step is simple:** call my office at **614-495-9658** and reference this letter to schedule a brief 10-15-minute initial phone consultation to start the process. You may also send me an e-mail to **michaelmoran@aresgrp.com**