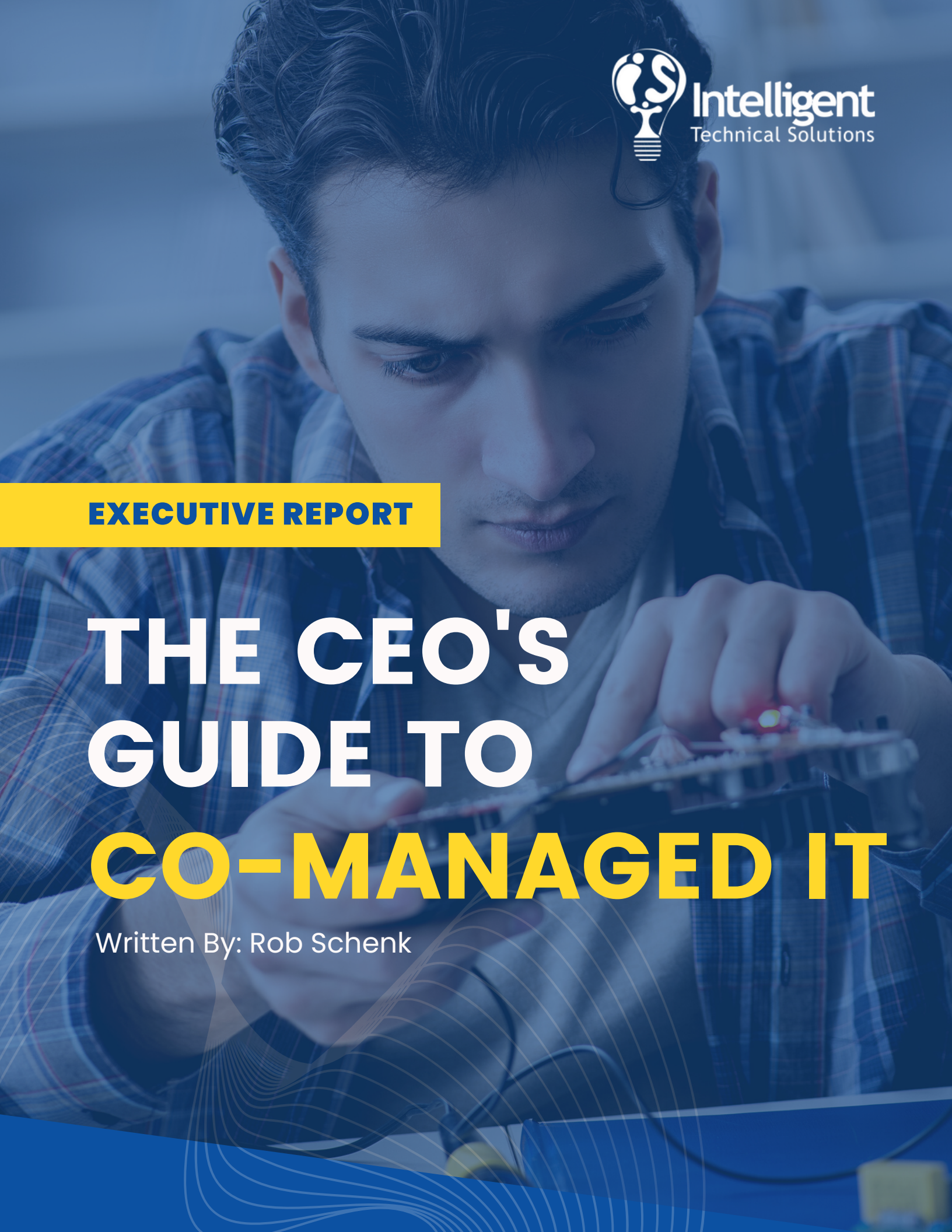


Intelligent Technical Solutions

EXECUTIVE REPORT

THE CEO'S GUIDE TO CO-MANAGED IT

Written By: Rob Schenk

THE DILEMMA

ALLOCATION OF FINANCIAL RESOURCES

CEOs and their executive teams repeatedly face tough investment decisions about where to allocate their limited financial resources.

Some of those decisions are more straightforward 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 are challenging to quantify and often don't easily secure a direct ROI. These investments involve Information Technology, and they are growing in number, breadth, and scope.

I.T. investments are more difficult to estimate, and the ROI or benefit might not be obvious or easily measured. In fact, you hope some don't produce a tangible ROI, like investing in cybersecurity and disaster recovery protection. However, no company can afford to accumulate technical debt in I.T. There's not a single department or function of your organization that isn't significantly controlled by, enhanced by, facilitated by, or outright dependent on I.T. And if your organization is NOT properly invested in cyber-protection and backup technologies, one cyber-attack or data loss event could have serious, long-lasting, and costly ramifications.

But no one has unlimited funds. So, what can be done about all of this?

Your IT Team is your backbone

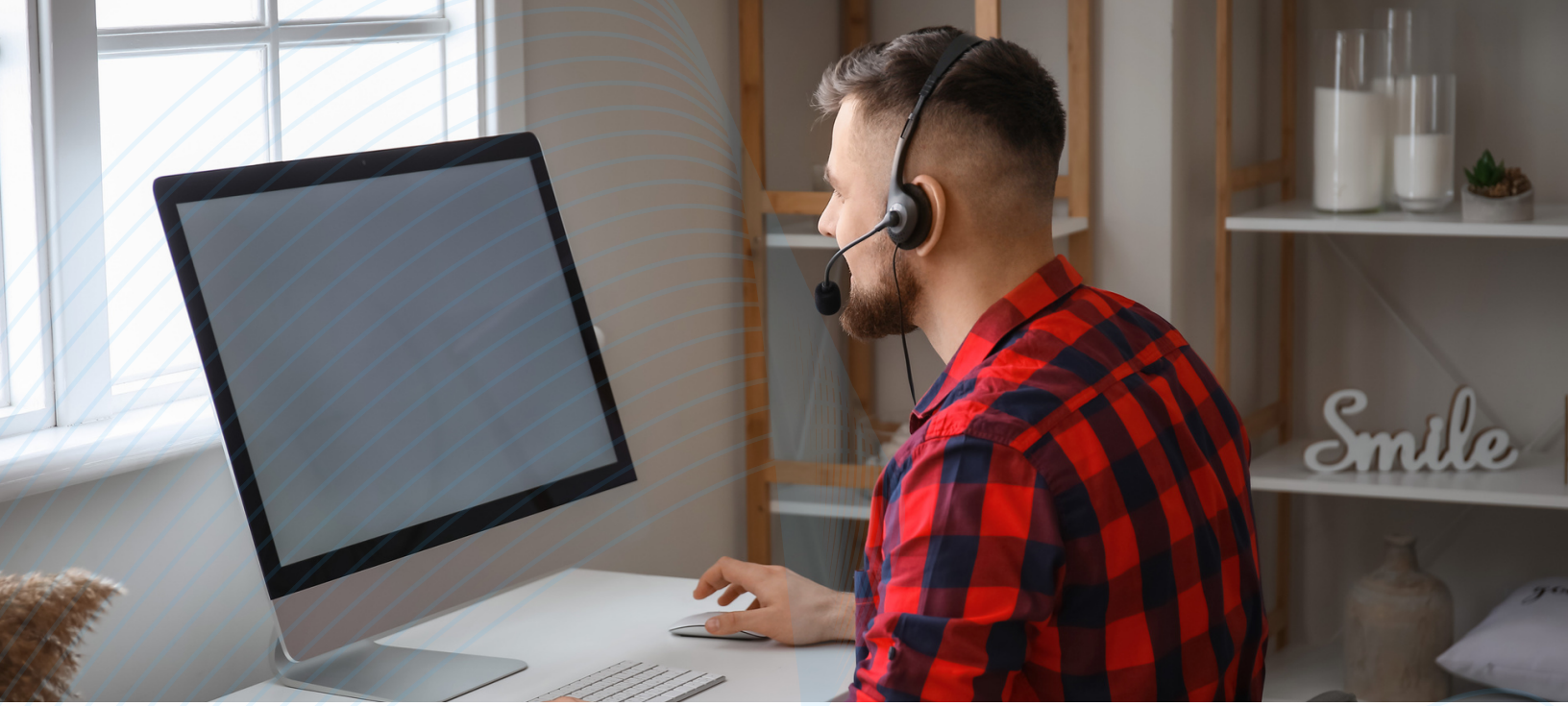
STRENGTHEN THEM

One option is to ignore it. Keep the status quo, make do with the I.T. staff and technology investments you have today and “hope” everything is going to be okay. Trust that your current I.T. department has it “handled.” Doing nothing is a choice, a Hobson’s choice that might result in catastrophic setbacks due to willful inaction. Companies, small and large alike, have experienced catastrophic setbacks by ignoring existing and worsening issues.

Your “catastrophic setback” might be a ransomware attack or a rogue employee who creates mayhem. 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. Or a well-meaning employee falls prey to a phishing scam and inadvertently transfers a large sum of money to a hacker or cybercriminal.

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

But suppose you are in a similar situation as most CEOs are when ITS San Francisco first begins working with them to deliver co-managed services. In that case, your I.T. 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 may also lack specialized knowledge about any number of things – data backup and disaster recovery, cybersecurity protections, secure cloud computing, complex database management, and more.



Your IT department may not be good at modeling technology costs, calculating expected returns on investment, or developing plans to leverage technology to address key business objectives.

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

The point is, your IT department may NOT be as prepared and capable as you may think to handle the rising complexity of IT systems for your growing company. The sophistication of cyber threats, coupled with your current resources, time, or event qualifications, can prove to be overwhelming and daunting.

If true, your organization **is at risk** for a significant IT failure.

To be crystal clear, in NO way am I suggesting your IT lead and staff aren't competent, dedicated, proficient, or hardworking people.

The fact is, NOBODY likes to go to the CEO with "bad news" or to constantly ask for more money or help, particularly if they were previously 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 trailing 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, shooing them along a path to failure.

EARLY WARNING SIGNS

YOUR IT TEAM NEEDS SUPPORT

For the reasons stated, conscientious IT leaders and team members often WON'T tell you they need more money, more staff, or 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 four early warning signs your IT team may need additional support:

THEY OFTEN WORK NIGHTS AND WEEKENDS

Everyone pulls an extended shift occasionally 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 and burning out without the CEO/CFO even knowing about it. This will end up hurting your organization

> "Today, tech has the highest employee turnover of any business sector".
>
> **INFORMATION WEEK IT NETWORK**

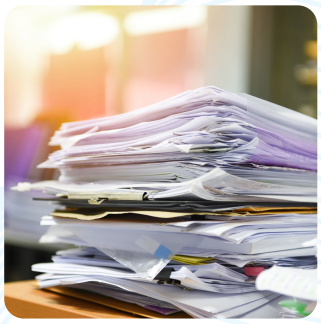
PROJECTS AREN'T DONE ON TIME OR CORRECTLY

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, or delivering promised benefits. 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.

YOU NOTICE DISTINCT BEHAVIORAL CHANGES

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.

PREVENTATIVE SECURITY MEASURES ARE STILL WHAT THEY WERE 2 YEARS AGO



Has your IT leader rolled out end-user security awareness training? Have they enforced the use of strong passwords? Do employees change their passwords routinely? Have they put together an Acceptable Use document or training to make sure employees know what is acceptable and what is not with company e-mail, Internet, confidential data, etc.? Have they provided you with updated network documentation and a comprehensive disaster recovery plan that has also been tested regularly?

If you've encountered any of these warning signs, you are not alone. All these pain points can be avoided with preventative maintenance and additional support. What you do not want to do is neglect or ignore your internal IT lead or department when they tell you they are overwhelmed and need additional support.

Many businesses find it very expensive to employ a fully staffed and diversely skilled team to run their IT operations. However, supplementing your IT by outsourcing the services not only cuts down those costs but also provides predictable monthly costs to cover the entire service. Partnering with ITS San Francisco allows you to make solid financial decisions to cover the entire service.

"ITS San Francisco has the perfect mix of sharp technical skills, a broad range of customer experience and a keen focus on customer service. They have been an invaluable resource."

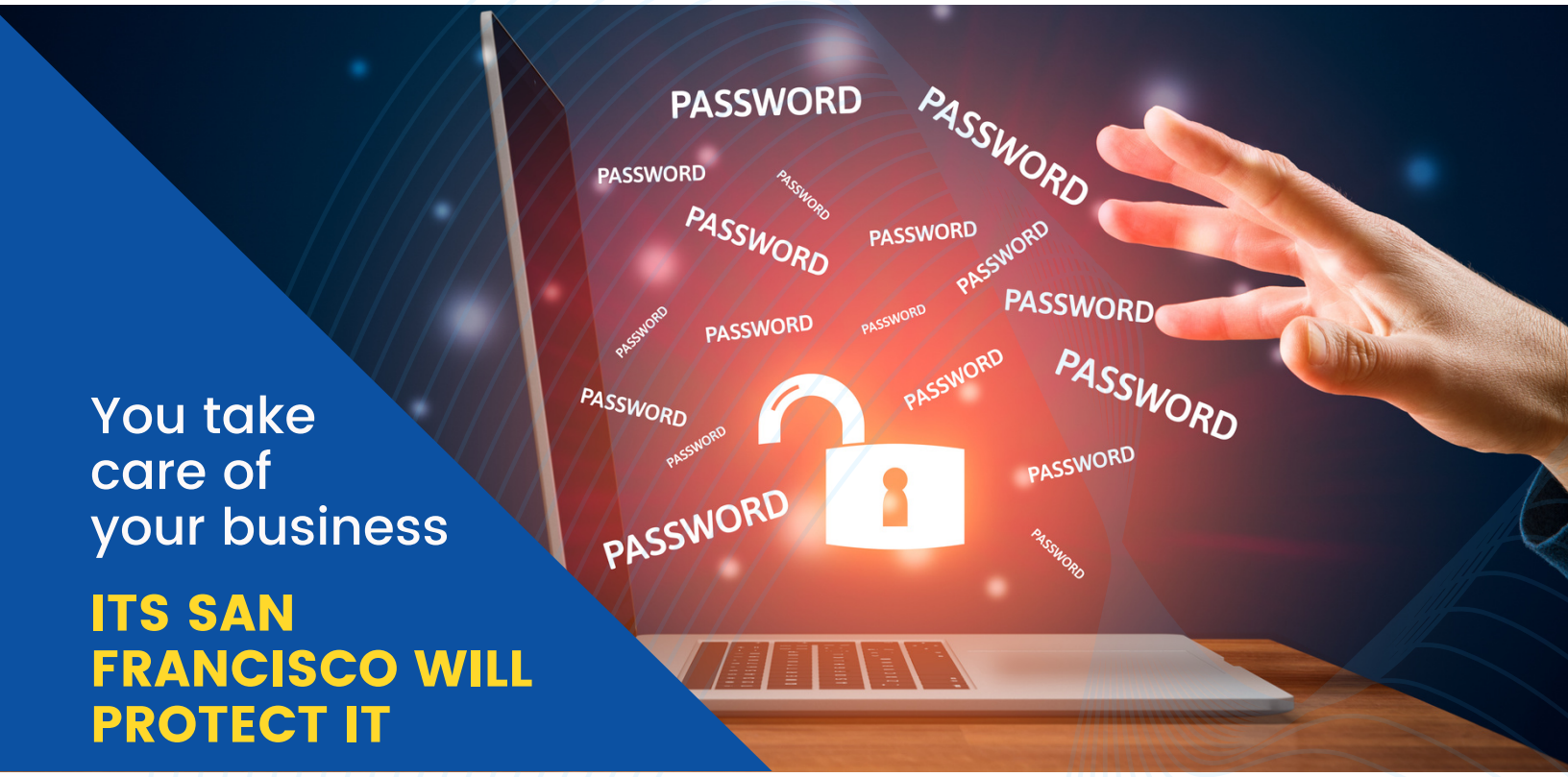
UNITED WAY OF THE BAY AREA,
A CO-MANAGED IT PARTNERSHIP

Your IT Team needs support

YOU ARE NOT ALONE

CYBERSECURITY GAPS

MAY BE YOUR BIGGEST VULNERABILITY



You take care of your business

ITS SAN FRANCISCO WILL PROTECT IT

Undoubtedly, an overwhelmed and understaffed IT department's greatest risk exposure is to an unexpected Cybersecurity incident. One incident can lead to data loss, extended downtime, and (potential) liability with a security breach or compliance violation.

What is the first thing that is left incomplete or overlooked when your IT department or lead is being pulled in 5 different directions at once? I would venture to guess it is cybersecurity improvements and preventative maintenance. Because cybersecurity defenses are often silent (triggering only to spurn cyberattacks or to fall victim to them), overworked IT staff may prioritize low-hanging fruit non-cybersecurity activities or ones with higher management visibility.

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

Cybercrime is up **600%** due to COVID-19

61% of phishing engagements resulted in a full compromise

To worsen matters, 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. Regardless of your organization's size or industry, these are areas you cannot ignore or undervalue.

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

43% of breach victims were small businesses

You'd be foolish to underestimate the cost and catastrophic 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 that their efforts are sufficient. Everyone in your company – and your clients – are depending on you.

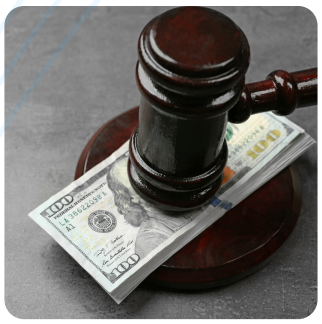
37% of credential theft breaches used stolen or weak passwords

IRREFUTABLE DAMAGE

LET US COUNT THE WAYS

REPUTATIONAL DAMAGES

When a breach happens, do you think your customers will rally around you? Have sympathy? This kind of news travels fast on social media. They will want 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 enough to alleviate those damaged by the breach?



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 more stringent 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 and any state regulating bodies.

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 are 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 in business, if that's even possible.

PAYING THE RANSOM

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 legal counsel's costs to help you respond to your clients and the media. Cash flow will be significantly disrupted, and budgets are 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.

Are you ready **TO HANDLE THREATS**

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 moment of poor judgment? Nobody believes they will be in a car wreck when they leave the house every day, but you still put the seatbelt on. You don't expect a life-threatening crash, but that's not a reason to not buckle up. What if?

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?

CO-MANAGED IT

HOW WE CAN SOLVE YOUR IT-RESOURCE DILEMMA

Because companies like yours face the dilemma of needing professional grade IT support but can't reasonably afford to invest in all of the tools, software, and staff required 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 we would limit your support to an "event" and then leave your team behind to try and support it.

It is a flexible partnership! We will customize a set of ongoing services and software tools specific to the needs of your IT person or department that fills in the gaps, supports their needs, and gives you far superior IT support and services at a much lower cost.

Here are the top reasons companies like yours of similar size and demographic 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 TO ADD TO YOUR HEADCOUNT.

Let's face it: overhead walks on two legs. Plus, finding, hiring, and retaining TOP talent is brutally difficult. With Co-Managed IT, you don't have the cost, overhead, or risk of a big IT team and department. 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 I.T. TEAM GETS INSTANT ACCESS TO THE SAME POWERFUL IT AUTOMATION & MANAGEMENT TOOLS WE USE

Let's face it: overhead walks on two legs. Plus, finding, hiring, and retaining TOP talent is brutally difficult. With Co-Managed IT, you don't have the cost, overhead, or risk of a big IT team and department. 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.

911 ON-SITE

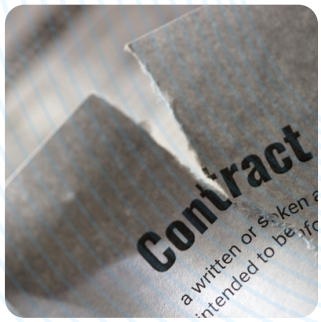
In an unexpected incident, your IT team is unable to perform their job, OR if a disaster were to strike, we would instantly provide support to prevent the wheels from falling off.

YOU GET A TEAM OF SMART & EXPERIENCED IT PROS

As a Co-Managed IT client, your IT team 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 ABOUT FALLING VICTIM TO A MAJOR CYBER ATTACK

We can assist your IT team in implementing next-gen cybersecurity protections to prevent or significantly mitigate the damages of a ransomware attack or security breach. We can also assist in providing end-user awareness training and help you initiate controls to prevent employees from doing things that would compromise the security and integrity of your network and data. CRITICAL MAINTENANCE WILL BE COMPLETED!



NO LONG TERM CONTRACTS

We're a flexible workforce you can expand and contract as needed.

CO-MANAGED IT

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 the help desk and end-user support but doesn't have the expertise in advanced Cybersecurity protection, line of business application upgrades, server maintenance, cloud technologies or 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.

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. In addition, your IT team could use a higher-level resource for intractable issues they can't resolve. Having an escalation resource available helps overall efficiency. We can train the trainer.

"Only 41% of cybersecurity professionals said their companies are utilizing best practices to ensure a secure remote workforce."

USECURITYMAGAZINE.COM
APRIL 2020

WE ARE NOT YOUR ADVERSARY

WE ARE YOUR ALLY

Although there are MANY benefits to Co-Managed IT services, this is certainly not a good fit for everyone. Here's a shortlist of incompatible organizations:

COMPANIES WHERE THE IT LEAD INSISTS ON VIEWING US AS AN ADVERSARY INSTEAD OF AN ALLY.

As previously stated, our goal is not to have you fire your IT lead or your entire I.T. staff. Our goal is a joint partnership that keeps your organization at the top of its game.

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.

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 IT leader's preferences, and we certainly will be flexible – we HAVE to be in order to make this work.

However, a big value we bring to the table is over 300+ years of accumulated expertise in supporting and securing computer networks. Therefore, the clients deriving the most benefit are ones that keep an open mind to looking at implementing our tools, methodologies, and systems, and adopting some of our best practices. Ultimately, this works best if it's a collaborative relationship.

But we cannot – will not – take on a client that is ignoring security best practices and good governance controls that we feel compromise the integrity and security of not only business operations but also of growth pursuits, team member well-being, and other core elements of a thriving company.

IF YOU ARE UNWILLING TO INVEST IN I.T.

As a leader and business owner myself, I relate to the need to monitor costs. However, starving an IT department of much-needed resources and support is short-sighted and risky.

Furthermore, some CEOs review 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, specialized skills, proven methodologies, and operational procedures.

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.

HOW CO-MANAGED IT SAVES YOUR ORGANIZATION MONEY

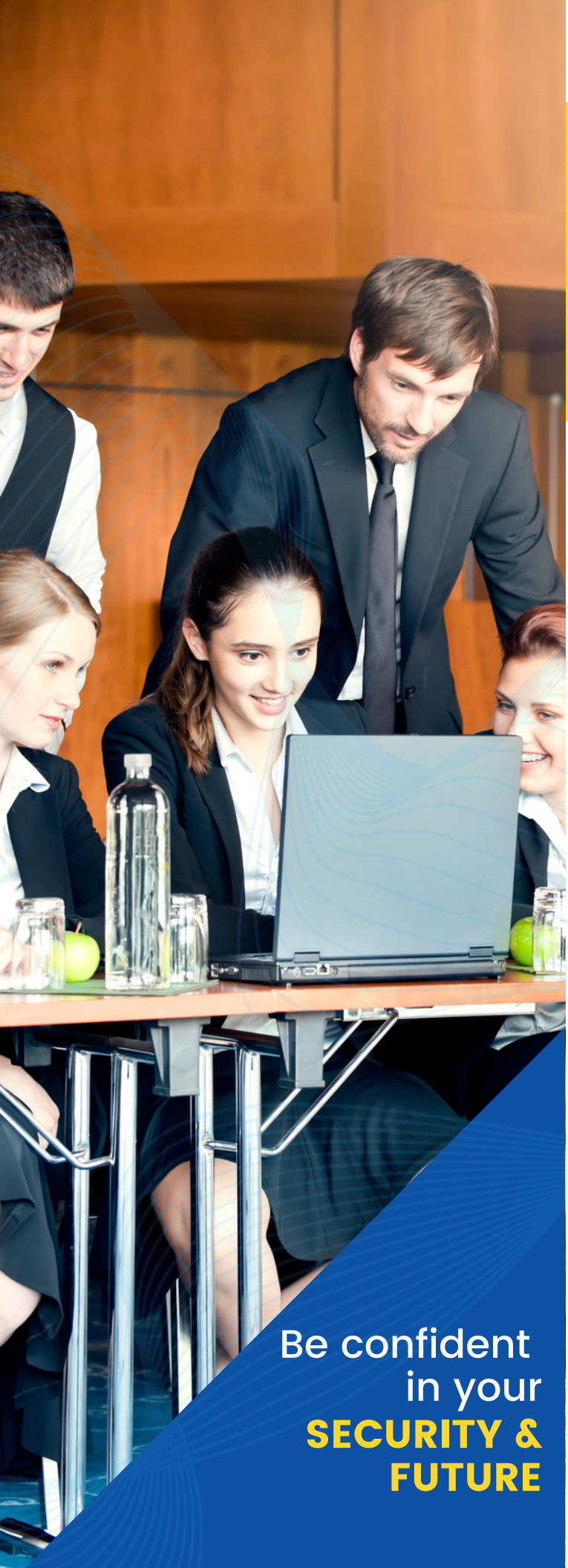
The Power of "We"
ACHIEVES IMMENSELY MORE

Many of your business decisions are guided by a cost versus profit analysis – it's usually the determining reason that companies embrace cloud technologies. Likewise, cost savings are also a common determinant for working with an MSP.

The economic benefits of outsourcing to an MSP have been analyzed. CompTIA conducted a survey of 400 businesses that began working with an MSP within the past year. The results indicate that 96% of respondents agree that Managed Services can save them a large amount of money annually.

What was the magnitude of cost reduction? 184 respondents reduced costs by 25% or more while 58 of the respondents had reductions of over 50%. In addition to the impressive reduction in costs, over 89% of respondents were very happy with the client experience and expertise their MSP delivered. Their reasoning for this response included security, positive support interactions, flexibility, and increased uptime.

There is no longer any reason for you to doubt the economic advantages associated with partnering with an MSP. Also, consider the collectively saved costs that accompany reduced accidental downtime. It's a safe bet that you'll realize financial benefits by Co-Managing your IT support.



WHAT TO LOOK FOR IN A CO-MANAGED IT PARTNER

We often see other IT firms in this space offer project-based support or monitoring-only services, ultimately aiming to take over IT for your entire company, likely resulting in jettisoning your IT lead or team.

These all-or-nothing options are neither optimal nor collaborative and may not deliver significant value for your IT investments.

If you have a productive, reliable IT leader or department, you ideally want to keep those people on your team, but just 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. Maximize your IT team's time—let a Co-Managed service provider handle routine maintenance and troubleshooting. You'll also benefit from additional support during peak demand periods, so your internal IT team doesn't have to stop working on major projects for small emergencies.

Secondly, 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.

These tunnel vision agreements are a waste of money unless you have a big IT team that just needs that tool – and if that's the case, you may be better off buying that software directly, or looking to compelling IT software packages available thru channel-only partners.

Finally, technical project work is often necessary, but you are going to get better results if your outsourced IT provider does not treat those projects as a "one-and-done" where they drop the solution in and take off, leaving your IT team to figure it how to maintain and optimize the solution over a long term.

A better approach is a Co-Managed IT environment when a solution is implemented by the same team that is supporting it. You'll gain access to a large, highly skilled IT department making it easy to get the expertise you need when you need it. IT teams are now an essential part of long-term business strategy. Our experts can help your company develop best-fit strategies that combine talent and technology to deliver measurable, reliable outcomes.

ITS SAN FRANCISCO IS UNIQUELY POSITIONED

TO DELIVER CO-MANAGED IT SERVICE

Success through **COLLABORATION**

There are many reasons ITS San Francisco is uniquely positioned to be your Co-Managed IT partner, starting with the simple fact we're the ONLY IT firm in the Bay Area offering solutions customized for Co-Management scenarios.

We are a partner you can TRUST. We're the team that will do what it takes to fix 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 quickly step in at any time.

We are an Award-winning MSP, recognized by CRN Magazine MSP Top 500, Clutch Top Bay Area MSPs, ChannelPro Top 100 Vertical Market MSP, Expertise Top San Francisco MSP, and a 2020 winner of the MSP 501 list from ChannelFutures. We currently serve over 50 businesses in the Bay Area and have a solid reputation for service built on over 300+ years' combined experience. But that's not all we do. We are also preeminent experts in Cybersecurity–thorough in our understanding of how to protect networks from data loss and ransomware, and how to leverage cloud technologies to drive efficiencies and higher team member productivity. Not to mention that our Customer Satisfaction ratings average over 98%, best in class in our industry.

We have invested heavily over 24 years in developing an efficient, robust, and responsive IT support system so you don't have to; instead, you just need to slot us in to solve your IT woes. The Co-Managed IT support we can wrap around you will dramatically improve and augment the effectiveness and quality of your IT team.

THINK CO-MANAGED IT IS RIGHT FOR YOU? OUR FREE ASSESSMENT WILL GIVE YOU THE ANSWER

If this report struck a chord and you want to explore how a Co-Managed IT relationship would benefit your organization, we've reserved initial telephone appointment times with our most senior leadership team to evaluate your specific situation and recommend the optimal Co-Managed IT approach for your specific needs, budget, and goals.

We work with your IT lead to identify problem areas that are opportunities for collaborative improvements such as:

1. inadequate or outdated Cybersecurity protocols and protections
2. insufficient backups
3. inconsistently-applied governance and unknown compliance violations
4. workloads that can be automated and streamlined for cost savings and more efficiency
5. insufficient (or no) documentation of IT systems and assets.

These are just a few of the most frequently discovered long-standing and challenging problems we find that many are surprised to learn 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 efficiency: the most common activities, activities consuming the most time, and how long and often they're saturated.
- 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? Are you prepared for the cost of a data breach recovery effort, which may include data privacy violation penalties?

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.

Click the link below to request this consultation.

Intelligent Technical Solutions