Special CEO Report

The CEO's Guide To Co-Managed IT

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

Provided By:

Mike Hughes
Network Titan

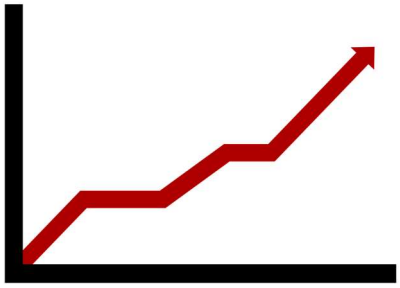
www.NetworkTitan.com
619-255-2621

The Dilemma: The Rising Costs Of IT And Cyber Security

Every day, CEOs and their executive teams are faced with tough investment decisions about where to allocate their 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 (which we'll define as all aspects of information technology, data protection, security and compliance), and they are growing in number, breadth and scope – and over the last several years have been steadily increasing at an exponential rate as cybercrime rages, more compliance regulations are introduced and IT talent is in short supply and expensive.



As you know, IT investments are more difficult to estimate, and the ROI or benefit might not be obvious or easily measured. In fact, you hope some investments NEVER produce a tangible ROI, like those in 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 technologies, a single cyber-attack or data-erasing event could have serious, long-lasting, costly ramifications – or even put you out of business. Today, insurance providers are putting stricter requirements on all companies to get cyber liability, crime or other policies that would cover the costs of a data breach or hack that severely impacts the business.

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

One option is to ignore it. Keep to the status quo, 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 or individual "has it handled." **But you have to know this is a perilous tightrope.** People in New Orleans trusted the dams and levees to hold – and they did – *until* they were hit with a Category 5 hurricane.

Your "Category 5" might be a ransomware attack that locks your entire company's data down, inaccessible even from your backup. It could be a rogue employee who intentionally sabotages your organization by deleting data or selling it to a competitor. It might be a failed server that went down, taking all its data with it, never to be revived again. It might be a corrupt SQL database that is beyond your current IT team's 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, documentation, cyber security protections, secure cloud computing, complex database management and more.

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

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

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

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

To be crystal clear, I'm NOT suggesting your IT lead and staff aren't smart, dedicated, capable, 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 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 That You May Be 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, 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 4 early warning signs that you may be pushing your IT department too hard:

1. **They're routinely working 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 after hours 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, the 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 items that often get 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.

This May Be One Of The Biggest Dangers You Face

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

As I 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 five minutes needing a password reset or needing help getting their e-mail, it's hard to tell that employee "No" because the IT team is 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 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 with "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 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, states each have their own data breach laws – and they are getting tougher by the minute. In California, complying with all the acronyms – CCPA, CPRA, SHRM - requires specialized skills and experience. If you're in health care

or financial services, you have additional notification requirements under the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA) Safeguards Rule, 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, **they 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 the California 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 the costs of specialized legal fees to help you respond to your clients and the media. Cash flow will be significantly disrupted, budgets blown up. And don't forget that California requires companies to provide one year of credit-monitoring services to consumers affected by a data breach.

   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 bestselling book *The Rockefeller Habits*.

   Harnish had $400,000 taken from his bank account when hackers were able to access his PC and intercept e-mails to 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 three 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? **You don't believe you will be in a car wreck when you leave the house every day, but you still put on the seat belt.** 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 all they do is use your server, website or profile to spread viruses and/or compromise other devices. If they hack you, they can relay spam, run malware, or promote their religious beliefs or political ideals.

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

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

GROWTH companies face the dilemma of needing professional-grade IT support but can't reasonably afford to invest in all the tools, software and staff this requires, which is exactly why we offer this new solution, 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 to support it (or give you the option of paying 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 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 in today's job market. 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 a family vacation or an illness, or when we have to 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-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.

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

- **You'll stop worrying (or worry less!) about falling victim to a major cyber-attack, outage or data-erasing event.** We can assist your IT leader in implementing next-gen 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.

- **We work directly with your IT leader.** They become more informed on critical topics such as cyber security, disaster recovery, compliance regulations, best practices and more.

- **NO LONG-TERM CONTRACTS.** We become a flexible workforce you can expand and contract as needed. Your IT team can scale up quickly and easily as your business grows and needs change.

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 help-desk 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 we fill in the areas where they need assistance.

Scenario 3: Your 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).

Who This Is NOT For:

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

- **Companies where the IT lead insists 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 – in order to make this work, we HAVE to be.

  However, a big value we bring to the table is our 17 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.

- **Organizations where the leadership is unwilling to invest in IT.**
  As a CEO myself, I completely understand the need to watch costs. However, starving an IT department of much-needed resources and support is foolish and risky. Further, some CEOs look at what they are paying us and think, "We could hire a full-time person for that money!" But they forget they are getting more than a single person – they are getting an ENTIRE team, a backup plan, tools and software, monitoring and specialized skills.

  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.

A Full IT Department At A Fraction Of The Cost

To understand how Co-managed IT saves you money and is a FAR superior choice to building your own IT department, you need to understand the structure and skill sets you'll require as a growing organization.

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

Title	Purpose	Employees	*Salary
Help Desk Technician (Levels 1-3)	Responsible for being the first line of defense to troubleshoot end-users' problems, questions and needs. Must be highly responsive.	1 per 70 employees	$50,000 – $60,000
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	$75,000 – $90,000
Network/Systems Engineer	Responsible for the strategic planning and implementation of the communication networks in your company.	1 per 200 employees	$80,000 – $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	The most senior technology executive inside of an organization. Responsible for setting and leading the IT strategy for the entire company to ensure IT facilitates the goals of the organization.	1	$140,000 – $200,000
CISO (Chief Information Security Officer)	Responsible for being head of IT security; creating, implementing and managing a company's IT security policies to prevent a breach; meeting compliance requirements and insurance security standards.	1	$200,000 – $250,000

*Southern California Averages

Additional IT Tools You'll Need:

- **Help desk ticket management system**
- **Remote management system**

What To Look For In A Co-Managed IT Partner

As mentioned above, 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 these options are not necessarily smart and won't deliver the 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 safely 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 your hired IT company drops the solution in and takes 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

There are several reasons our company is uniquely positioned to be your co-managed IT partner, starting with the simple fact that we have a long history with our co-managed clients.

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 work with clients that employ anywhere from 1 to 3 or more full-time IT personnel. They typically support from 50 to hundreds of users. We have many more companies we work with who are happy to advocate for Network Titan and are willing to talk with you.

We have more than 15 clients that have been with us for at least 10 years. We believe that being in the IT and Cyber Security industry and having a long list of tenured clients is something to be proud of. Read some of our client reviews in the attached list.

The Network Titan team is well known and respected for our fast response and expertise. We currently serve over 75 businesses in Southern California and have a 5-star reputation for service built on our 17 years of experience. *But that's not all we do*. We are also at the top of our field in cyber security and network protection from data loss, breaches and ransomware. We are preferred

for cloud migrations and cloud solutions, compliance and line-of-business software expertise for Law Firms, Accounting, Engineering, Med/Bio Tech, Life Sciences, DoD, and Manufacturing.

We have invested many thousands of dollars and over 17 years in developing the most efficient, robust and responsive IT support system so you don't have to. The Co-managed IT support we provide will dramatically improve your effectiveness and the quality of your IT team.

What Do Other CEOs In Southern California Say?

https://www.NetworkTitan.com/testimonials/

Visit our website and read our client reviews… Hear firsthand why Network Titan has a 5-star reputation for providing excellent IT Support and Cyber Security protection.

Think Co-Managed IT Is Right For You? Our Free Diagnostic Consultation Will Give You Answers

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

We work with your IT leader to determine areas that are lacking and 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 I have sufficient redundancy and documented systems and processes in my IT department to avoid a single point of failure?**

- **Am I overspending and not getting my money's worth in any aspect of our IT?**

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

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

To request this consultation:

1. Go online to www.networktitan.com/consultation-request
2. Call me directly at 619-255-2621 ext. 101
3. E-mail your appointment request to jerald@networktitan.com

One Important Request

We STRONGLY encourage you to bring your IT leader 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 that we 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 leader 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.

Sincerely,

Mike Hughes
President and CEO
Network Titan

PS – If you would like to speak with any of our CEO clients who are utilizing our Co-managed IT services, please e-mail me at mike@networktitan.com or call me at 619-255-2621 ext. 101 and I'll arrange for you to speak with them directly.

A Friendly, Local Team That Responds Quickly and Efficiently to Your IT Needs.

The greatest single benefit of having Network Titan handle our IT services is that we are very hands off. I can let Mike and his team know what we need and they just get it done. This allows our company spend time focusing on our clients without having to worry about our network systems. **Network Titan has removed a huge burden from my business day and has allowed me to put more attention to my business.**

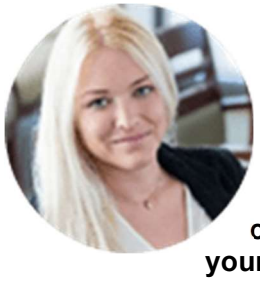
Danny Barnett
Chief Financial Officer at Nova Services

Outstanding Customer Service No Matter Time or Location.

Working with Network Titan is like having your own in-house IT department but only better. Mike and his team are focused on providing outstanding customer service no matter the time or location. Simply put, they're outstanding! Network Titan is incredibly responsive and technically sound. They consider your business to be their own. **It's hard to go wrong with Network Titan. They provide a responsive, cost-effective solution to all your IT needs.**

Jim Buechler
President & CEO at Cutwater Spirits

Network Titan Makes Us A Priority.



"It is hard to pick just one benefit seeing as Network Titan is the best IT firm we could wish for. We are consistently impressed with the after-hours support, follow through on all requests, prompt responses and support. Network Titan makes us a priority. Although they have many clients, we always know they are available to us, regardless of time or day. Working with Network Titan gives us a peace of mind. We know we can always count on them. **Don't wait for the IT catastrophe to happen, get ahead of it with Network Titan. With them on your team, you will have a great team on your side."**

Victoria Switzer
Director of Accounting at Gomez Trial Attorneys

This Company Will Build A Long-Lasting Relationship.

Network Titan is trustworthy, fair and always available. Their response time is incredible. **When a problem arises and a computer is down they get the problem solved incredibly fast.** Network Titan is always there for you when you need them and is looking to build a long-lasting relationship.

Robert Burner
President at American Sheet Metal