

THE I.T. MONEY PIT

5 Ways Mac-based Businesses Waste Thousands Of
Dollars On I.T. And Still Don't Get The Functionality,
Security And Support That They Need



CREATIVE RESOURCES
TECHNOLOGY GROUP



CREATIVE RESOURCES
TECHNOLOGY GROUP

The I.T. Money Pit

5 Ways Mac-based Businesses Waste Thousands Of Dollars On I.T. And Still Don't Get The Functionality, Security And Support That They Need

After conducting hundreds of I.T. assessments for small to midsize enterprises in Southern California and Central Texas, we've uncovered 5 areas where companies routinely spend hundreds of thousands of dollars on I.T. yet still struggle with recurring problems, downtime, ineffective systems and security risks.

This report will show you exactly where money is leaking out of your organization and being wasted on I.T. systems and software that are old, unnecessary and putting you at risk, and what to do about it now.

Provided By: Creative Resources Technology Group

Author: Russell Poucher

10200 US-290, Suite 206, Austin, TX 78736

www.creativeresources.net

(877) 622-7911





About The Author



Russell Poucher, President and founder of Creative Resources Technology Group, takes pride in the knowledge that his firm is committed to providing top tier technical support, customer service and product knowledge to his customers. Russell Poucher helps his clients navigate the challenging world of information technology (IT) and cybersecurity. This allows them to focus on their organization's core competencies, keeping their entire infrastructure operational and fully efficient. Russell's passion for security and IT resulted in launching Creative Resources Technology Group. (CRTG). Since 1996, CRTG has evolved into the premier Apple managed services, professional services and cybersecurity company in Southern California, and later followed by the locations in Central Texas.

Prior to starting CRTG, Russell worked as a System Administrator for several leading pre-press firms in Orange and Los Angeles Counties. He has numerous certifications in networking, security and system administration with a specialty in the Apple platform. By combining his knowledge of the Manufacturing, pre-press and creative industries, Russell is able to provide fully integrated technical solutions to his customers. Since opening its doors in 1996, CRTG has been heralded for its unique blend of technical expertise and customer service.

CRTG is a trusted advisor to businesses, providing Mac-based solutions, technical expertise and resources to help its clients achieve their goals and solve their IT problems that other service providers cannot. The guiding principles and core values that Russell holds closest to his heart are also upheld by the company: Open and honest communication, taking extreme ownership, working in an efficient and focused manner and gratitude for the opportunities that have been provided.

Russell, a national speaker, has shared the stage with some of the top speakers in the cyber security (Kevin Mitnick) and information technology (IT) ranks (Steve Jobs, Richard Branson) at some of the premier Apple events (MacTech, MacWorld). As a writer and content developer, he has written books and training curriculum on topics from macOS to Windows, security, infrastructure and WiFi networking. He has been recruited by Apple (curriculum development, training and speaking), Adobe (curriculum development and speaking) and Dell (securing down their macOS environment, internationally) over the last 18 years to help with several initiatives and projects, including: writing curriculum for Apple's technical certification classes, being an Apple Certified Trainer, contracted as an Apple Professional Services provider and overseeing the training of Apple Consultants from Southern California and Central Texas.

Notice: This publication is intended to provide accurate and authoritative information in regard to the subject matter covered. However, no warranties are made. It is provided with the understanding that the author and the publisher are NOT engaged in rendering legal, accounting or related professional services or advice and that this publication contains opinions of its author. This publication is NOT intended as a substitute for specific legal or accounting advice for any particular institution or individual. The publisher accepts NO responsibility or liability for any individual's decisions or actions made as a result of information or opinion contained herein.



The I.T. Money Pit:

5 Ways Businesses Waste Money On I.T.

Even in the best of times, no business wants to have money secretly “leaking” out of their organization due to waste, poor management and a lack of planning.

But when it comes to I.T., **most CEOs don’t even know what they’re spending money on, much less if they’re making smart investments to minimize cost and waste.** It’s the proverbial “money pit,” a “black hole” of cost that they are unable to accurately assess.



Like a malnourished obese person, they are consuming FAR more calories than necessary, but still not getting the micronutrients they need. Businesses are often in the same situation with I.T. – **they are spending thousands of dollars, but are still not getting the speed, performance, security and productivity they need.**

As Andy Grove, former CEO of Intel, said, “Only the paranoid survive.” In our experience, most CEOs are **not paranoid enough when it comes to loss prevention and I.T. waste.** That’s why we wrote this report.

My team and I have found millions of dollars in dysfunctional I.T., SaaS bloat, unnecessary software, productivity-killing systems and under appreciated cyber risk – even in generally well-run companies led by respected executives.

In fact, there has yet to be a client we’ve helped in the 25+ years we’ve been providing I.T. support and services that has not produced at least \$100,000 in fast savings. Not **ONE**.

As you read this report, know that this IS very likely going on in your organization. As you go through this, know that what follows are only five of the most common areas where we see waste occurring. When we do a deeper analysis, we often find several other areas that need attention. Please take a look at everything below and know there IS a different path you can take – and one you should look into sooner rather than later.



#1: “Maverick” Spending, No Strategy And Undisciplined Planning

Many companies we’ve audited have a mishmash of patchwork technology pieced together like an old Frankenstein monster lumbering along. Nothing makes sense, nothing works as efficiently as it should, and the entire I.T. system is awash in inefficiencies, duplicate and redundant resources and outdated technologies – all adding up to thousands of dollars wasted, unnecessarily, that could be put to better use in the business OR simply added to bottom-line profitability.

Do you have a veritable technology “junk drawer” full of equipment, wires and software that nobody can identify or explain and that does nothing but suck up space and precious resources?

In our audits of I.T. environments, we almost always uncover multiple servers, switches and other devices – all of which they are paying to support and back up – that could easily be consolidated and upgraded to deliver faster performance, more reliability and more security.

Over time, different cooks in the kitchen have added pieces and patched problems with Band-Aid after Band-Aid instead of strategically designing the whole to maximize productivity and lower the total cost of ownership by using more up-to-date (and lower-cost) cloud technologies.

In fact, most of the C-suite executives we’ve interviewed do not know what they even have and are paying for. I.T. is a giant black hole of spend that nobody can justify.



That’s why the first step in understanding how to lower your overall I.T. costs and get a far better ROI is to conduct a deep audit of your entire environment to look for:

- Redundant machines, servers and devices.
- Duplicate SaaS applications your company is paying for (see “SaaS Bloat”).
- Out-of-date software that’s putting your organization at risk for a cyber-attack.
- Old servers that could be consolidated and moved to the cloud for greater speed and availability, easier access and team collaboration and productivity.
- Backup systems you’re paying for that are unreliable and inconsistent.



At CRTG, we help clients avoid wasted IT spend and hidden risks by conducting a comprehensive **IT Environment Audit**. Our process identifies redundant systems, unnecessary SaaS subscriptions, and outdated technology that can expose organizations to cyber threats or reduce productivity. From there, we consolidate, modernize, and optimize infrastructure — often moving workloads to the cloud — while ensuring reliable, tested backup systems are in place. This approach not only lowers overall IT costs but also increases ROI, performance, and security for our clients.

Case Study: Reducing IT Costs Through a Strategic Audit

Background

A mid-sized professional services firm was struggling with rising IT costs and inconsistent system performance. Employees were frustrated with downtime, while leadership was concerned about security risks and low ROI from their existing investments.

Challenge

Our audit revealed several issues:

- Redundant devices and servers that were no longer necessary.
- SaaS bloat — multiple departments paying for duplicate applications.
- Unpatched, out-of-date software creating cybersecurity vulnerabilities.
- Aging on-premises servers that slowed collaboration and remote access.
- Unreliable backup systems that left the firm exposed to potential data loss.

Solution

CRTG delivered a step-by-step remediation plan:

1. Consolidation of servers and devices to reduce overhead and maintenance.
2. Rationalization of SaaS licenses, cutting duplicate costs and renegotiating contracts.
3. Software lifecycle management, updating or retiring outdated tools.
4. Migration to a secure cloud environment for improved speed, accessibility, and collaboration.
5. Implementation of a reliable, tested backup and recovery system aligned with compliance requirements.



Outcome

- 25% reduction in IT operating costs within the first year.
- Stronger security posture, eliminating multiple vulnerabilities.
- Improved productivity and collaboration through cloud adoption.
- Peace of mind knowing backups were consistent, tested, and reliable.

Key Takeaway

By starting with a thorough audit, CRTG helped the client transform their IT from a cost center into a strategic advantage — lowering expenses while boosting performance, security, and ROI.

#2: SaaS Bloat

In the era of cloud- and subscription-based everything, it's easy for small and midsize businesses to accumulate software-as-a-service (SaaS) subscriptions without a clear inventory or strategy.

Employees often purchase tools independently and outside of the I.T. budget (also known as “shadow I.T.”) to get their job done. Because these subscriptions are in small amounts, and because most companies don't routinely audit these purchases, most companies are unnecessarily spending thousands of dollars in duplicate and unnecessary SaaS applications.

Here are some stats that speak to this point:

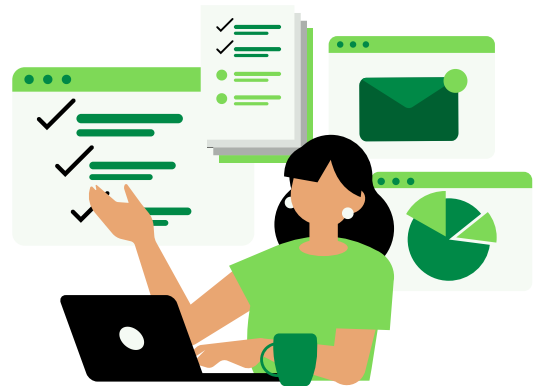
- A 2023 Productiv SaaS Trends report found that the average midsize company uses 254 SaaS apps, **yet only 45% of those licenses are actively used.**
- According to Gartner, organizations overspend on SaaS by at least 30% due to poor management of licenses and subscriptions.
- Flexera's 2023 State Of ITAM Report states that 49% of companies identify “identifying unused or underused software” as a top cost-optimization priority.

Let's say your business uses 100 SaaS apps at an average of \$25/month per user, and only half are actively used. That's \$1,250/month (\$15,000/year) in waste for a 10-person team – and that's being conservative.



We also routinely find:

- Businesses are paying for full-feature enterprise plans when a basic tier would suffice.
- Companies fail to revoke and/or cancel licenses after employees leave or when the licenses are no longer needed.
- Employees have multiple software tools that do the same thing (e.g., three project management platforms, two virtual meeting and communication tools, multiple CRM systems, etc.).



Part of our service for clients is to conduct a quarterly audit of all SaaS subscriptions so they can be reviewed to determine if they are still needed or can be consolidated, downgraded or simply eliminated, which saves thousands of dollars and closes another door a hacker can crawl through to gain access to your network.

Left unchecked, SaaS bloat silently drains your I.T. budget and wastes money that could be going directly to your bottom line. Trimming even 10% to 20% of this waste can free up thousands for higher-payoff investments.

We typically help our clients save \$625 to \$950, per month, just in consolidation of their SaaS applications while giving them visibility into what's being spent.

In fact, one client saw dramatic results after we applied this process.

By performing our quarterly SaaS subscription audit, we identified redundant applications spread across multiple departments, uncovered licenses that were no longer being used, and consolidated several overlapping tools. As a result, this client was able to streamline operations and cut unnecessary costs.

The outcome? They saved nearly \$250,000 this year alone, money that would have otherwise been wasted on unused or duplicate subscriptions. Beyond the financial impact, eliminating unnecessary applications also reduced their exposure to potential cyber threats, since every extra login and SaaS portal represents another door a hacker could exploit.



#3: Grossly Inadequate Data Compliance And Cybersecurity Protections

While you might not think of spending money on cybersecurity as a “cost savings,” you would do a complete 180 if you ever experienced the massive expenses associated with a ransomware attack or breach.

When A Cyber-Attack Happens, The Losses Stack Up And Multiply While Sales Tank.

Right away, there’s an instant loss of productivity. At best, you’re crippled. In the worst cases, you’re completely shut down, unable to transact, unable to deliver the promised products and services to clients and unable to operate. In other cases, thousands if not millions of dollars are drained directly from your accounts without any chance of recovery.

Then you have the loss of critical data, reputational damage, potential lawsuits and government fines. **The epicenter of this disaster lands DIRECTLY on YOUR desk for YOU to deal with** – a problem that WILL significantly undo your best-laid plans for growth and progress.

Yet, despite this, we have found that most companies we’ve audited are GROSSLY unprepared and unprotected from a ransomware attack or other major cybersecurity event EVEN THOUGH they have invested heavily in I.T. staff and resources. Before we showed them irrefutable evidence of these inadequacies, the CEO was convinced that “I.T. has it handled.” A ticking time bomb they didn’t know was “live” under their seat.



Let me also point out that many insurance companies now require you to have a robust cybersecurity plan and protocols in place in order for you to be insurable. And with new data-protection laws being introduced and implemented on both a federal and state level, you may have clients coming to you to demand you show proof of adequate cyberprotections or they will be unable to do business with you. Do you really want to wait until you have the proverbial “gun to the head” need to get this enacted?

At CRTG, we have an entire team dedicated to solving this for our clients so they can have complete peace of mind knowing they are truly protected. One recent example: a multi-location healthcare provider came to us after their cyber liability insurance renewal was denied because their policies and safeguards didn't meet updated carrier requirements. Within 90 days, we conducted a full risk assessment, implemented multi-factor authentication across all systems, rolled out an advanced endpoint protection suite, and trained their staff in phishing awareness. The result? They not only secured the insurance coverage they needed but also earned a premium reduction for demonstrating stronger compliance. Even more importantly, their executive team now has the assurance that their organization meets both regulatory standards and client expectations.

#4: Chronic I.T. Problems, System Failures And Slow Response To Problems

Yet We Find That Most CEOs Don't Realize Just How Often Their Employees Are Being Interrupted And Distracted Due To Recurring I.T. Failures Because It's “Hidden” From Them.

As the saying goes, “Overhead walks on two legs.” Any leader knows that unproductive, distracted workers not only kill profitability but increase the chances of mistakes, missed deadlines, sloppy work and low morale. A frustrated team is not a productive one.

After our audit, many CEOs are shocked to discover their employees are dealing with chronic I.T. problems that are constantly getting in the way of serving clients, closing sales and doing their job, forcing them to stop what they are doing, redoing the work they just spent hours doing or possibly NOT doing what they are supposed to do.

Just one hour of this a day adds up when multiplied over an entire year and your entire workforce. As an example, one client we audited discovered each employee was wasting an average of 3 hours per month dealing with tech support issues – a STAGGERING amount of time wasted, not only in lower productivity, but also in the help-desk costs they were paying their Mac I.T. company to handle all the support tickets being submitted. A DOUBLE WHAMMY of needless costs and profits going down the drain.



After coming onboard, we got that down to 30 minutes per month – one tenth of the time.

In the majority of the situations where this is happening, I.T. is being outsourced to an organization that is not as responsive as they should be and has not been strategic or proactive in upgrading systems to avoid these costs.

To make matters worse, many support tickets are submitted by employees into a “black hole” without a guarantee of resolution or response time – so they’re left waiting for HOURS, unable to work, simply because their outsourced I.T. company is not getting back to them quickly.

Problems occur again and again, and frustrated employees end up finding a work-around or attempt to fix it themselves because it’s less frustrating than sitting on their hands waiting for a tech to call them back and fix the problem.

All the while, the company is paying their outsourced Mac I.T. company to resolve all of this – but they’re only compounding the problem.

At CRTG, our average response time to most issues is within an hour. That means our clients aren’t left waiting while problems disrupt their operations. Whether it’s a critical system outage, a security alert, or a simple day-to-day IT request, our team is ready to respond quickly and effectively. Fast response times not only minimize downtime but also build confidence that issues will be resolved before they can escalate into costly disruptions.

#5: Delaying Necessary Upgrades Until Systems Fail

With inflation and costs on the rise, it’s no surprise CEOs and CFOs try to stretch I.T. systems upgrades until they are absolutely necessary – but there is a false economy in waiting too long.

Older systems not only become slower and less effective, but they also require more maintenance and support, increasing service fees. Old systems can also fail without notice, forcing you to upgrade without proper planning, incurring emergency support costs, data recovery fees and unplanned downtime.



One client learned this lesson the hard way. They decided to delay a critical server upgrade, believing it would “save money” in the short term. A few months later, that outdated system failed during peak business hours, bringing their operations to a standstill. Instead of the predictable cost of an upgrade, they were suddenly faced with an emergency recovery bill that was nearly three times higher, not to mention the revenue lost during days of downtime.

After the incident, they partnered with CRTG to modernize their infrastructure, and they’ve since told us they wish they had invested in the upgrade from the start. Today, they enjoy the peace of mind that comes with proactive planning, knowing they won’t be caught off guard again.

In many cases, data loss can occur if systems fail unexpectedly – and upgrading old legacy systems may require expensive specialists who can migrate the data and functions to a newer system. Then there’s the increased risk of a cyber-attack since older systems tend to be less secure and may no longer be supported by the vendor.

Done right, upgrades could have been done in smaller, budgeted increments over time, making it easier on the company from a budgetary perspective and in disruption of productivity.

This is why, at CRTG, we track and document all of the equipment, software and systems your Mac-based business owns, giving you visibility into what’s actually going on, what truly needs to be upgraded and when, giving you a budget...



Is Your Current Mac I.T. Company Allowing You To Waste Money, Break The Law And Incur Risk?

Take This Quiz To Find Out

If your current Mac I.T. company does not score a “Yes” on every point, they are NOT adequately protecting and serving you. Don’t let them “convince” you otherwise and DO NOT give them a free pass on any one of these critical points. Remember, it’s YOUR business, income and reputation on the line.

- ☐ **Do they meet with you quarterly to review your current I.T. spend and map out future upgrades so you can appropriately budget for I.T. spend?** Or do they wait until an upgrade is on fire and then send you a big, expensive quote for a critical upgrade you didn't budget or plan for?
- ☐ **Have they met with you recently – in the last 3 months – to specifically review and discuss what they are doing NOW to protect you from ransomware and the latest cyber-attacks?** This should be a routine report provided with the quarterly strategy meeting mentioned above.
- ☐ **Do they track and report on how many support tickets your team is submitting?** Is it under 2 per month per employee? If it's higher than that, what are they proposing to eliminate recurring problems your employees are constantly having to deal with?
- ☐ Have they proposed ways to **consolidate and eliminate SaaS bloat** in your organization?
- ☐ **Have they ever asked to see your cyber liability insurance policy?** Have they verified they are doing everything your policy REQUIRES to avoid having a claim denied in the event of a cyber-attack?
- ☐ **Do THEY have adequate insurance to cover YOU if they make a mistake and your practice is compromised?** Do you have a copy of THEIR CURRENT policy? Does it specifically cover YOU for losses and damages?
- ☐ **Have you been fully and frankly briefed on what to do IF you get compromised?** Have they provided you with a response plan? If not, WHY?



- ☐ Have they told you if they are outsourcing your support to a third-party organization? **DO YOU KNOW WHO HAS ACCESS TO YOUR I.T. SYSTEMS AND THE DATA IT HOLDS?** If they are outsourcing, have they shown you what security controls they have in place to ensure that a rogue technician, living in another country, would be prevented from using their free and full access to your network to do harm?
- ☐ **Do they have controls in place to force your employees to use strong passwords?** Do they require a PASSWORD management system to prevent employees from using weak passwords? If an employee is fired or quits, do they have a process in place to make sure ALL passwords are changed? Can you see it?
- ☐ **Do they provide employee training so your staff knows how to utilize the tools they have instead of buying additional software and tools you don't need?**
- ☐ **Have they recommended or conducted a comprehensive risk assessment every single year?** By law, you're required to do this, and your I.T. company should be handling the I.T. part of that for you.
- ☐ **Have they implemented web-filtering technology to prevent your employees from going to infected websites or websites you DON'T want them accessing at work?** I know no one in YOUR office would do this, but why risk it?
- ☐ **Have they given you and your employees ANY kind of cybersecurity awareness training?** This is now required by law for many industries and by insurance companies as a condition of receiving coverage.
- ☐ **Have they properly configured your e-mail system to prevent the sending/receiving of confidential or protected data?**
- ☐ **Do they offer, or have they at least talked to you about, dark web/deep web ID monitoring?** There are new tools available that monitor cybercrime websites and data for YOUR specific credentials being sold or traded. Once a leak is detected, this tool notifies you immediately so you can change your password and be on high alert.



Ready For Efficient I.T. Services That Don't Waste Your Money And Put You At Undo Risk?

Because you're a prospective client, I'd like to offer you a **FREE I.T. Systems And Security Assessment** to demonstrate how we could put the ideas in this report to work for you and dramatically improve the value you are getting for your I.T. spend, eliminate waste and reduce your exposure and risk to a devastating cyber-attack.

The next step is simple: Call my office at **(877) 622-7911** and reference this report to schedule a brief 10- to 15-minute initial consultation.

On this call we can discuss your unique situation and any concerns you have and, of course, answer any questions you have about us. If you feel comfortable moving ahead, we'll schedule a convenient time to conduct our proprietary (and **FREE**) **I.T. Systems And Security Assessment**.

This Assessment can be conducted with or without your current Mac I.T. company or department knowing (we can give you the full details on our initial call).

At the end of the Assessment, you'll know:

- Where you are overpaying (or getting underserved) for the I.T. services, tools and support you are paying your current Mac I.T. company to deliver.
- Whether or not your company is truly protected from hackers and ransomware, and where you are partially or totally exposed to a devastating, extremely expensive cyber event.
- If your data is actually being backed up in a manner that would allow you to recover it quickly in the event of an emergency or ransomware attack. (Hint: Most backups are NOT.)
- How you could lower the overall costs of I.T. while improving communication, security and performance, as well as the productivity of your employees.

Fresh eyes see things that others cannot – so, at a minimum, our free Assessment is a completely cost- and risk-free way to get a credible third-party validation of the security, stability and efficiency of your I.T. systems.



Sign Up For Your **FREE Assessment At Our Website:**

www.creativeresources.net/freenetworkassessment

**If you prefer, you can also e-mail me at r.poucher@creativeresources.net or
call me direct at (877) 622-7911**

Please don't be "too busy" and set this aside to deal with it later. If you have even a sneaking suspicion that money is being wasted and you are at risk for a cyber-attack, every minute counts.



Here's What Our Clients Have To Say:



Perfect in Every Way! Creative Resources designed and installed every aspect of our multi-location integrated system to manage our diverse business activities. We have high value investment assets and were handicapped by inadequate IT. Creative Resources did everything we could have wanted in a highly professional manner. We now have a thoroughly integrated system where every aspect fits exactly the need we explained at the outset. They now maintain the system and are immediately responsive and 100% effective. They stand out by providing consistent, prompt, and quality customer service. The team is extremely knowledgeable, professional, friendly, and most importantly, put their client's best interests first!

**-Barry Meguiar, Founder,
Revival Outside the Wall**



The tasks of maintaining and fixing our systems are no longer there –offloaded to CRTG so we can be more productive doing what we do. CRTG is proactive in maintaining our systems and preventing problems. They always offer the best solution, not just a quick fix. CRTG is very responsive and knowledgeable with the new technology available. Set up a meeting with Russell, he's a great guy and easy to work with - and so is the rest of his staff.

**-Alex Selamat, President,
Creative Fusion**



The biggest benefit in partnering with CRTG is getting better services that fits our business needs. It is also the service that CRTG provides. There are situations that occur daily and we can count on CRTG for providing professional support that is consistent since Day 1. CRTG is equipped with up-to-date technology and continues to provide strategies to guide us on our overall IT direction. If someone was on the fence about choosing an IT firm, I would tell them, to choose CRTG because we've had nothing but good experiences.

**-Jane Wan, President,
Quality Worldwide**



Here's What Our Clients Have To Say:



The biggest benefit we have is knowing that when there is a problem CRTG has a big team behind us that will get it straightened out ASAP. Although we are just a (sole practitioner) we have from day 1 years ago, been treated as a customer who is very important to CRTG. I love the fact that they remote into my machine from their base office. I don't have to wait for a technician to come out. They are available to us on Saturdays and Sundays. In the past I worked with a company who, if they got a request from a larger company, they would cancel our appointment. CRTG has never done that, in all the time I have been associated with them. Try them. They treat you the same on the 100th call as on the first call when you were a new client. If you are as impatient as I am when you need help on your computer, you will not be disappointed.

**-Suzanne Mellor, Exec. Support,
General Dynamics**



CRTG has provided us a better sense of a secure environment. Their proactive approach to security and network stability is what they do best. Give CRTG a try if you want quick responses to security and stability issues. We no longer have to worry about our IT issues, instead we can focus on what we do best in the medical field. We know that CRTG has us covered.

**-Matthew Krall, Controller
Oasis Medical**



I'm so grateful for the Apple Consultants Network leading us to CRTG. I no longer worry if an IT issue arises because I have complete confidence that CRTG will solve any and all issues promptly and effectively, so we won't continually have the same issues. I love that we have an IT Strategist to interact with to make sure our needs are met. Our needs have not only been met since day one, but CRTG's professionalism and service has far exceeded our expectations. They are friendly, responsive, knowledgeable, accessible, and most importantly, they add a touch of personal care which is typically not associated with most IT firms that offers a wide range of services like they do. I highly recommend this company.

**-Jeff Elghanayan, President,
Bicoastal Properties.**