



A JUMP START TECHNOLOGY GUIDE

BEFORE YOU SIGN

What 25 years of office moves have taught me about technology risk. The essential infrastructure questions every business should answer before committing to new office space.

Ron DeAngelis

President, Jump Start Technology

JUMP START TECHNOLOGY

550 S Winchester Blvd. Suite 600, San Jose, CA 95128

650-949-0667 | ron@jumpstarttech.com | jumpstarttech.com

In 25 years of supporting Bay Area businesses through office moves, I have never seen a company struggle on move-in day because they hired the wrong movers or picked the wrong paint color.

Every operational failure I have witnessed traces back to the same moment: the lease signing. Specifically, to what was not asked before it happened.

Internet that is not ready. Electrical that cannot support the load. A "server room" that is a closet. A building with exclusive carrier agreements and no alternatives. None of these are technology problems. They are due diligence failures, and they are almost entirely preventable if you know which questions to ask, and when to ask them.

The when matters. After you sign, your options narrow considerably.

Here is what that looks like in practice.

A medical device company signed a lease in a building that advertised "high-speed internet available." What that meant was shared cable service capped at 100 Mbps. Their video meetings with East Coast partners were unreliable from day one. Upgrading to dedicated fiber required a substantial building investment and months of delay.

A professional services firm moved into a beautifully renovated historic building. After move-in, they discovered the electrical capacity could not support their network equipment, security appliances, and workstation load simultaneously. An unexpected electrical upgrade delayed occupancy and increased costs significantly.

A growing startup assumed the "server room" noted in the lease would be adequate. It was a converted storage closet, with no cooling, no redundant power, and no physical security. Instead of expanding infrastructure as planned, they were forced to redesign their network and shift more services to the cloud earlier than anticipated.

None of these were technical failures. They were due diligence failures. The questions that could have prevented them take less time to ask than negotiating parking ratios. Most companies simply do not realize those questions need to be raised before the lease is finalized.

The good news: these risks are predictable. They show up in the same places, every time.

Here is the moment most leaders do not recognize until after the fact. The moment you sign a lease, you are also locking in connectivity options, carrier access, electrical capacity, equipment placement, and physical security constraints. Those decisions shape how your team connects, collaborates, and protects information for years.

Most companies today are cloud-first. They may not run large servers onsite. But they still depend on reliable connectivity, secure network infrastructure, properly designed wireless coverage, and sufficient power for core systems. When those elements are constrained by the building, the impact shows up in productivity and frustration. Not as a single crisis you can fix, but as daily friction you learn to live with.

The companies that move smoothly are not the ones with the biggest IT budgets. They are the ones that asked better questions earlier.

What follows is what we have learned after decades of seeing both outcomes: the questions that prevent expensive surprises and protect your team from unnecessary disruption. You do not need to become a technology expert to make a good real estate decision. You simply need to know which infrastructure questions should be answered before you commit.

PART 1

Internet Connectivity: The Most Critical Question

Everything else in this guide depends on this section. Electrical problems are expensive. Cabling problems are disruptive. Internet problems are existential. A modern business that cannot connect reliably cannot operate, and unlike most infrastructure problems, internet limitations are often baked into the building in ways that are difficult or impossible to remedy after you have signed.

QUESTION 1

What internet service providers actually serve this building, and what does "fiber available" really mean?

"Fiber available" is one of the most misleading phrases in commercial real estate. It can mean a building has multiple carriers with existing infrastructure and competitive pricing. It can also mean a carrier is willing to run fiber to the building if you pay for it, a process that takes three to six months and costs \$10,000 to \$50,000 before you have connected a single device.

The question to ask is not whether fiber is available. It is which carriers have physical infrastructure in the building right now, whether there are exclusive agreements limiting your options, and what the installation lead time is for each carrier. Exclusive agreements deserve particular scrutiny. A building with a single-provider exclusive means you will pay whatever that carrier charges with no leverage and no alternatives, for the length of your lease. That is a constraint worth knowing about before you fall in love with the space.

QUESTION 2

What speeds are actually available, not theoretically, but today?

A building can have fiber infrastructure and still deliver inadequate bandwidth to individual tenants. Speeds are sometimes capped per tenant regardless of the underlying infrastructure. More commonly, bandwidth is shared across multiple businesses in the building, which means performance degrades during peak usage hours, precisely when you need it most.

The baseline numbers worth knowing: a small office of five to ten people needs a minimum of 100 Mbps and preferably 250 Mbps. A growing business of ten to thirty people needs 250 to 500 Mbps minimum. Larger

operations need 500 Mbps to a gigabit. If your work is video-heavy or involves large file transfers, plan for more. Ask for a sample service agreement and current pricing before drawing conclusions. What is advertised and what is delivered are not always the same thing.

The line that matters most: if you rely on cloud applications, video conferencing, or large file transfers, you cannot upgrade your way out of building limitations after you have signed. The ceiling is the ceiling.

QUESTION 3

What is the redundancy situation, and does the building support it?

A single internet connection is a single point of failure. For businesses where downtime means your team cannot work, you lose revenue, you miss client deadlines, or you damage client relationships, and that description covers most businesses operating on cloud-based applications today, redundancy is not optional. It is the difference between an outage being an inconvenience and being a crisis.

Redundancy means a secondary connection from a different carrier using a different physical path into the building. Both conditions matter. Two connections that share the same physical infrastructure fail together. Before signing, confirm whether a secondary carrier can be installed, whether different carriers use genuinely separate physical paths, and whether there are any building restrictions on backup connectivity. Budget for it from day one rather than treating it as a future upgrade, because the future upgrade conversation usually happens in the middle of an outage, which is the worst possible time to be negotiating with a carrier.

PART 2

Electrical and Power Infrastructure

Technology requires power, and not just adequate power, but clean, reliable, dedicated power with room to grow. This is the infrastructure problem that surprises people most often, because electrical capacity is invisible during a building tour and rarely comes up in lease negotiations until something goes wrong.

QUESTION 4

What is the electrical capacity allocated to this suite, and is it enough?

Buildings designed decades ago were not built for the power demands of a modern office. Workstations, dual monitors, servers, network equipment, charging infrastructure, kitchen appliances, it accumulates faster than most people expect. The question is not just whether the building has power. It is whether it has enough dedicated power for your specific load, and whether that capacity is yours alone or shared with other tenants.

The math is worth doing before you commit. Each workstation with a computer and dual monitors draws 3 to 5 amps. A network equipment rack draws 10 to 20 amps. A small server rack draws 20 to 30 amps. A kitchen or break room draws 15 to 20 amps. Add those up against your planned layout and compare to the suite's available amperage. If the numbers are close, find out whether additional circuits can be added and what that costs. If the building cannot support your load and has no upgrade path, that is a constraint you will live with for the length of your lease.

Ask specifically about circuit panel configuration and whether capacity is dedicated to your suite or shared. Shared electrical capacity means another tenant's peak usage affects yours, a problem that is difficult to diagnose and impossible to fully solve after you have signed.

QUESTION 5

What happens to your operations when the power goes out?

In the Bay Area, this is not a theoretical question. PG&E public safety shutoffs, rolling blackouts, and unexpected outages are real operational risks. The question is not whether an outage will happen. It is whether you will be prepared when it does.

Start by finding out what the building's generator backup actually covers. The answer is frequently limited to emergency lighting and elevators, which protects people but does nothing for your equipment or your operations. If you need to keep systems running through an outage, and if power loss means data loss, lost revenue, damaged equipment from improper shutdowns, or missed client commitments, building generator coverage alone is not enough.

What you want to know is whether you can install your own uninterruptible power supply equipment and whether there are any building restrictions on battery backup systems. UPS infrastructure protects against both outages and the power fluctuations that damage equipment silently over time. It is not an extravagance for most businesses. It is operational insurance, and it is significantly easier to plan for before move-in than to retrofit into a space that was not designed to accommodate it.

PART 3

Physical Space for Technology Infrastructure

Technology equipment needs a home, and not just any available closet. Network gear generates heat, requires ventilation, needs secure access, and needs to stay connected to the rest of the building's infrastructure. Whether the space you are evaluating has an appropriate place for that equipment, and where that place sits relative to the building's network architecture, has a direct effect on your build-out costs and your long-term operational reliability.

QUESTION 6

Is there a dedicated server room or network closet, and is it actually suitable?

The existence of a "server room" on a floor plan does not tell you much. We have seen converted storage closets with no cooling, no dedicated power, and no physical security listed as server rooms in lease documents. What you are looking for is a climate-controlled, separately secured space with adequate electrical capacity and proper ventilation, one that was designed for equipment, not repurposed from something else.

The practical minimums: temperature maintained between 65 and 75 degrees, humidity below 50 percent, 15 to 30 amps of dedicated electrical capacity, a separate lock or access control independent from the rest of the suite, and enough physical space for rack-mounted equipment plus cable management. If the space does not meet those conditions, find out whether you can modify it and what that costs. Retrofitting an inadequate room

into a proper equipment space typically runs \$10,000 to \$30,000 depending on what is required. That number belongs in your build-out budget before you sign, not as a surprise after.

QUESTION 7

Where are the building's main network connection points, and how far is your suite from them?

This question requires a brief explanation of terminology that most non-technical people never encounter: buildings have one or more main distribution frames (MDF), the central point where outside network connections enter the building and distribute internally, and intermediate distribution frames (IDF) on individual floors that connect back to the MDF. Your suite needs to connect to one of these, and the distance between your space and the nearest connection point directly affects your cabling costs.

Cable runs are priced per drop, typically \$50 to \$150 each, and a typical office needs dozens of them. If your suite is on a floor with its own IDF, cabling is straightforward and relatively inexpensive. If the nearest connection point is three floors away with no existing cable pathways, you are looking at a significantly different number, and potentially at the cost of creating new pathways through the building's infrastructure.

If you are evaluating multiple spaces in the same building, this is worth asking about each one. All else being equal, the suite closer to the MDF or IDF will cost meaningfully less to wire, a difference that rarely comes up in lease negotiations but shows up clearly in your first contractor quote.

PART 4

Existing Infrastructure and Cabling

The space you are evaluating has a history. Previous tenants left cabling behind, conference rooms may or may not have been wired for modern use, and the building may offer WiFi that sounds convenient but rarely is. Understanding what is already there, and what condition it is in, can save you \$5,000 to \$20,000 in build-out costs, or reveal expenses that need to be factored into your decision before you commit.

QUESTION 8

What network cabling already exists, and is it actually usable?

Existing cabling is only valuable if it meets current standards and terminates where you need it. The minimum acceptable standard is Cat 5e, which supports gigabit speeds. Cat 6 or Cat 6a is preferred, supporting multi-gigabit and 10-gigabit speeds. Anything older than Cat 5e is effectively worthless for modern use and will need to be replaced regardless.

Even cabling that meets the standard may not match your layout. Drops that terminate in the wrong locations, or a previous tenant's configuration that does not align with your planned floor plan, mean new runs regardless of what is there. Before signing, ask to see documentation of the existing cabling infrastructure and get quotes for any additional drops you will need. Cable installation after move-in is disruptive and expensive. It is far better to know the real number upfront and negotiate accordingly.

QUESTION 9

Are conference rooms pre-wired for AV and connectivity?

A conference room with four walls and a table is not a conference room in 2026. Modern meeting spaces need network drops for video conferencing, dedicated power for laptops and displays, HDMI or display connections for screen sharing, and appropriate mounting infrastructure for cameras and audio equipment. If those elements are not already in place, you are building them from scratch after move-in, which is both expensive and disruptive.

The costs add up faster than most people expect. Network drops run \$150 to \$300 per room. HDMI and display runs add \$200 to \$400. Additional electrical runs \$300 to \$600. Video conferencing equipment mounting adds \$500 to \$1,500. A typical office with three or four conference rooms can easily require \$5,000 to \$10,000 in AV infrastructure build-out that was not in anyone's original budget.

If rooms are not pre-wired, get those numbers before you sign. They belong in your total occupancy cost calculation, not in a surprise invoice six weeks after move-in.

QUESTION 10

What is the WiFi situation, and can you install your own?

Some buildings provide shared WiFi as an amenity. It is almost always inadequate for business use. Shared bandwidth, inconsistent coverage, no security segmentation from other tenants, no control over configuration or prioritization. It is fine for a lobby. It is not a substitute for a properly designed wireless network.

What you want is your own wireless infrastructure: multiple access points sized to your square footage, roughly one per 2,000 to 3,000 square feet, ceiling or wall mounted, with network cabling run to each location. What you need to confirm is whether the building allows it. Some buildings restrict ceiling-mounted equipment, limit where cabling can be run, or require building approval for wireless installations that can delay your timeline.

If the building restricts your ability to install your own wireless infrastructure, treat it as a serious red flag. Strong, reliable WiFi is not optional for a modern office, and a building that prevents you from achieving it is making a fundamental technology decision on your behalf.

PART 5

Building Access and Logistics

Technology infrastructure does not install itself. Network equipment needs to be racked, cables need to be run, server rooms need to be configured, and systems need to be tested before your team arrives. That work takes time, typically one to two weeks for a properly planned installation, and it has to happen before your official move-in date. Whether the building accommodates that reality is worth knowing before you sign.

QUESTION 11

How far in advance can you access the space for technology installation, and on whose schedule?

Early access is not just a convenience. It is a prerequisite for day-one functionality. A small office under 15 people needs a minimum of three to five days. A mid-size office between 15 and 40 people needs one to two weeks. A larger operation needs two to three weeks, sometimes more depending on infrastructure complexity.

The access question has two parts. The first is timing: when can you get in. The second is flexibility: can your IT vendors access the space independently, are installations restricted to evenings or weekends, and are there permits or building approvals required before work can begin. Some buildings are straightforward. Others layer on restrictions that compress your installation window in ways that do not become clear until you are trying to coordinate a cabling crew, a network equipment delivery, and a furniture installation simultaneously in the week before move-in.

If the building will not provide adequate early access, you are not just accepting inconvenience. You are accepting that your team's first week in the new space will include technology that is not fully operational.

QUESTION 12

What are the restrictions on equipment delivery and installation, and what do they cost?

Buildings have rules about how and when equipment moves in. Freight elevator reservations, delivery hour restrictions, loading dock time windows, move-in fees, certificates of insurance for vendors. In isolation, none of these are unreasonable. In combination, in a busy urban building, they can make coordinating technology installation with furniture delivery genuinely difficult.

The specific thing to watch for: buildings in dense areas sometimes have severe loading dock restrictions, with morning delivery windows only, advance reservations required weeks out, and strict time limits that do not account for how long technology installation actually takes. If your cabling crew and your furniture vendor are competing for the same freight elevator on the same day because the building will not accommodate separate windows, someone is waiting and your timeline is slipping.

Get all of this in writing before you sign. If the restrictions are too onerous to work around, negotiate better terms. And if building management is defensive or dismissive about reasonable logistics questions during the evaluation process, that is worth paying attention to. It is a preview of what problem-solving looks like after you are locked in.

PART 6

Security and Physical Protection

Most conversations about technology security focus on what happens over a network. This section is about what happens in the room.

Your technology equipment represents a significant physical investment, often \$50,000 to \$200,000 or more for a mid-size office. More importantly, it contains or provides access to your business data. The same risks you manage digitally can also walk through a door, and the building you choose either supports your ability to control that or it does not.

QUESTION 13

What are the building's physical security measures, and can you supplement them?

Start with the basics: is there controlled building access, or is the lobby effectively open to the public? Is there security camera coverage? How is suite access managed, with keys, access cards, or biometric? Is there 24/7 security or only business hours coverage, and what are the after-hours access procedures for your own team?

Those questions establish the floor. The more important question is whether you can build on it. Can you add independent access control to your suite? Can your server room or network closet be separately keyed or secured from the rest of the space? In buildings where the answer to both of those is no, you are dependent entirely on the building's security posture, which may not align with your own.

If you handle sensitive data in financial services, healthcare, or legal services, your compliance requirements may set a higher bar than the building's standard offering. Verify that before you sign, not after your first audit.

QUESTION 14

Is there environmental monitoring, and what happens when something triggers after hours?

Technology equipment fails when exposed to heat, humidity, water, or power problems. A server room that hits 90 degrees overnight because the HVAC failed, or a network closet that takes on water from a pipe above the ceiling, these are not rare scenarios. They happen, and the damage they cause is almost always worse than it needed to be because no one knew until morning.

Find out whether the building has environmental monitoring for temperature, humidity, and water detection in equipment areas. Ask whether there are alerts for HVAC failures and what the response protocol is if something triggers outside business hours. If the building does not provide monitoring, you can install your own. Sensors and alerting systems are relatively inexpensive. But it is significantly easier if the building's infrastructure supports integration rather than working around it.

The threshold worth knowing: equipment rooms should stay between 65 and 75 degrees with humidity below 50 percent. An alert at 80 degrees gives you time to respond. No alert at all means you are finding out about the problem when equipment starts failing.

PART 7

Cybersecurity and Compliance: The Hidden Infrastructure Risk

Most businesses think of cybersecurity as a software problem. Firewalls, passwords, endpoint protection, cloud security tools. What they do not think about is the building. In 2026, that is a gap with real consequences.

Your physical office environment affects your security posture more directly than most leaders realize. If your network equipment sits in an unsecured telecom room, if your internet connection is shared across tenants without proper segmentation, or if you cannot control who has physical access to your infrastructure, you are not just accepting operational risk. You may be creating compliance exposure, affecting your insurance eligibility, and taking on liability you do not know you have assumed.

QUESTION 15

Who actually has physical access to your network infrastructure?

Many buildings place tenant internet handoffs and fiber connections in shared telecom rooms, spaces accessible to building management, other tenants, contractors, and cleaning crews. Before signing, find out whether the telecom room is shared, who has access, whether that access is logged or controlled, and whether you can secure your own equipment in a locked cabinet within that space.

If you handle financial data, healthcare information, legal records, intellectual property, or government contracts, uncontrolled physical access to your network infrastructure is not a minor concern. It may be a compliance issue. And even if you are not in a regulated industry, shared unsecured infrastructure is unnecessary risk with no upside.

QUESTION 16

Is building-provided internet truly isolated from other tenants?

Some buildings offer shared or managed internet as a convenience. It is worth understanding exactly what that means before you rely on it. Is connectivity shared across tenants? Are networks fully segmented? Can you install your own firewall and maintain control over your network perimeter? Are there restrictions that would prevent you from bringing in an independent carrier if the building's solution does not meet your security requirements?

Most security-conscious businesses deploy their own firewall regardless of what the building provides. The question is whether the building allows it, and whether you have confirmed that before signing rather than after.

QUESTION 17

Will this space support your cyber insurance requirements?

This is the question almost no one asks during a lease evaluation, and it is becoming increasingly important. Cyber insurance providers now scrutinize infrastructure decisions. Depending on your coverage, they may expect redundant internet connectivity, secure equipment placement, environmental monitoring, and documented disaster recovery planning. If the building cannot support those requirements, if you cannot install a secondary carrier, secure your equipment properly, or add monitoring systems, you may have a coverage problem you do not discover until you need to file a claim.

It is far easier to confirm building compatibility with your insurance requirements before you sign than to retrofit under pressure after an incident.

PART 8

Future-Proofing, Scalability, and How Your Team Actually Works

The space you choose today needs to support how your business operates two or three years from now, not just on your average Tuesday, but on your busiest day. Most office planning defaults to average usage. Average headcount, average bandwidth consumption, average conference room demand. That is the wrong

baseline. Infrastructure that handles average load comfortably often fails under peak conditions, and in hybrid environments, the gap between average and peak is wider than it used to be.

QUESTION 18

What does peak occupancy actually look like, and can the infrastructure support it?

Before evaluating a space, get clear internally on your real numbers. How many people will be onsite on your busiest day? Are desks assigned or shared? How many simultaneous video calls happen at once? Are collaboration areas carrying more load than individual workstations?

Hybrid schedules compress attendance into fewer days, which means your busiest days are busier than they would have been in a traditional five-day office. WiFi density, bandwidth, and conference room capacity all need to be sized for that reality, not for a smoothed average. If the space cannot support peak demand, you will not fix it with furniture rearrangement.

QUESTION 19

Are conference rooms truly video-ready, and can the building support what that requires?

Modern conference rooms need reliable bandwidth, strong WiFi, adequate power, proper AV cabling, and appropriate camera and microphone placement. These are not enhancements. They are baseline requirements for a hybrid workforce. Retrofitting them after move-in is expensive and disruptive.

Verify this before you sign. A room with a screen on the wall is not a video-ready conference room.

QUESTION 20

What is the capacity for expansion and technology upgrades over the life of the lease?

Think three to five years out. If you are growing, assume you will need two to three times your current bandwidth, fifty percent more power capacity, additional network infrastructure, and expanded wireless coverage.

What is the maximum internet bandwidth the building can deliver, not what you are buying initially, but the ceiling? Is there spare electrical capacity? Can you add network drops after initial installation? Are there limitations on equipment expansion? If the building cannot support reasonable growth, you may face another disruptive move sooner than expected. That cost, operational and financial, rarely shows up in lease comparisons, but it should.

PART 9

Smart Buildings, Costs, and Timeline Reality

Newer buildings increasingly advertise smart capabilities: app-based access control, connected HVAC, occupancy sensors, tenant experience apps. These features can improve day-to-day experience. They also introduce network considerations that are worth understanding before you sign.

The core question is not whether smart building systems are good or bad. It is whether they are isolated from your network. Building systems and tenant networks should be completely separate. If a building system requires access to your internal infrastructure, or if the answer to that question is vague, press harder. You do not need to manage the building's systems. You just need to ensure your network remains independent and secure.

QUESTION 21

What technology costs are your responsibility versus the landlord's?

This is where expensive misunderstandings happen most often. The general breakdown: landlords typically cover building internet infrastructure to the suite demarcation point, base electrical to code minimums, and building HVAC. Tenants typically cover all cabling within the suite, additional electrical beyond the base build-out, their own equipment, and any upgrades required for their specific needs.

The gray areas, including server room improvements, additional electrical capacity, network infrastructure upgrades, and access control enhancements, are worth negotiating explicitly. In a competitive leasing market, landlords sometimes contribute to technology build-out costs. Always ask. Get the answer in writing.

QUESTION 22

What is the realistic timeline for getting internet and technology infrastructure operational?

"Fiber available" does not mean "fiber ready on your move-in date." Installation timelines are consistently longer than expected, and you cannot operate without connectivity.

Realistic Bay Area timelines: an existing building fiber connection runs four to eight weeks from order to installation. A new fiber build to a building with no existing infrastructure runs three to six months, sometimes longer. Network cabling installation runs one to three weeks depending on scope. Electrical upgrades run two to six weeks depending on complexity.

Order your internet service the day you sign the lease. Not when move-in feels close. Not when the buildout is nearly done. The day you sign. Internet installation delays are the single most common cause of move-in chaos, and they are entirely avoidable with early action.

Before You Sign: Do Your Due Diligence

You have asked all the questions. Now verify the answers before you commit.

Visit the space during business hours. Run speed tests if building WiFi is provided. Find the network closet. Check electrical outlet placement and quantity. Verify what is actually in the conference rooms. Talk to current tenants about internet reliability and how building management responds when something goes wrong.

Get everything in writing. Verbal commitments during the leasing process are not commitments. "We can definitely get you fiber," "early access will not be a problem," "we will contribute to your build-out costs," if it is not in the lease or a signed addendum, assume it is not happening. If they will not put it in writing, that tells you something important.

Have your IT provider walk the space before you sign. A 30-minute evaluation catches problems that are not visible during a standard tour: inadequate electrical capacity, poor network infrastructure, access restrictions, environmental issues. It costs almost nothing relative to what it can prevent.

What 25 Years Actually Teaches You

The companies that move well are not the ones with the largest IT budgets or the most sophisticated technology teams. They are the ones that understood, early enough to act on it, that a real estate decision and a technology decision are often the same decision.

That is the lesson that repeats. Not a specific technical failure or a particular building problem, but the consistent gap between when infrastructure decisions get made and when the people who understand infrastructure get involved.

By the time most businesses bring their IT provider into an office move conversation, the lease is signed, the timeline is fixed, and the options are narrowed. What is left is execution under constraints that did not need to exist.

The questions in this guide are not complicated. They do not require technical expertise to ask or to evaluate. They just need to be asked at the right moment, before you commit, not after. That window is shorter than most people realize. And it matters more than almost any other decision you will make about your new space.

After You Sign: What Happens Next

If you have worked through these questions and you are ready to move into execution, we created The Office Move IT Checklist as a practical companion. It covers everything from four to six months before your move through post-move adjustments, including a Day 1 Staff Guide for your team.

Download The Complete Office Move IT Checklist

The step-by-step companion to this guide, from planning through move-in day.

Questions About Your Specific Move?

If you are evaluating office space right now and would value a direct conversation about what to look for, I am happy to talk.

No presentation. No proposal. Just a focused discussion about your specific situation and what may require attention before you sign.

Ron DeAngelis

President, Jump Start Technology
650-949-0667 | ron@jumpstarttech.com
jumpstarttech.com

