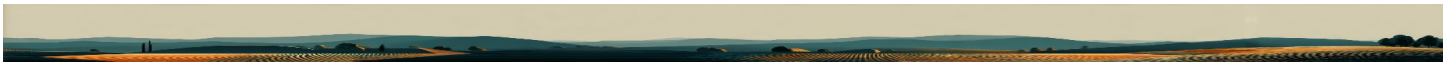
LATTIS

Is Your Business Ready for a Disaster? Most Aren't.

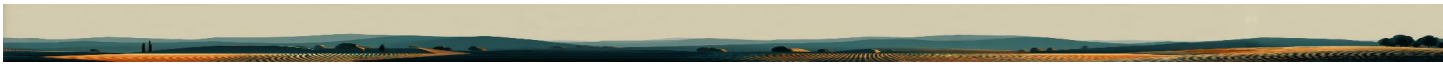
A plain-English guide to disaster recovery for business owners

April 2026



LATTIS

Lattis · Atascadero, CA · lattisnetworks.com



LATTIS

Introduction

I've walked into businesses after disasters. A ransomware attack that encrypted everything. A server that failed with no working backup. A phone system that died and couldn't be resurrected because the parts don't exist anymore. In every case, the pain was real and the cost was significant. In most cases, it was preventable.

Disaster recovery isn't about preparing for a plane hitting your building. It's about preparing for the things that actually happen — human error, cyberattacks, hardware failure, extended power outages, a fiber cut on the street. This guide walks through what a real DR plan looks like for a small or mid-size business, and what you can do right now to be less exposed.

What Counts as a Disaster?

Human Error

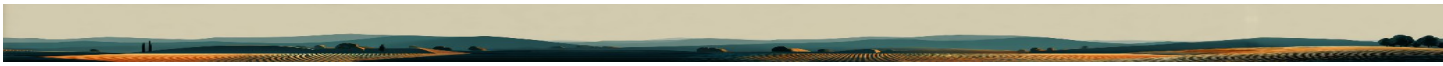
Accidental deletion. Misconfiguration. Someone doing something they shouldn't have had access to do in the first place. Human error is the most common cause of data loss and system outages — and the probability is higher than most people think. It's also the most preventable, with proper access controls, change management, and backups that actually work.

Cyberattack

Ransomware, data theft, business email compromise. This is the most expensive and most common serious disaster for small and mid-size businesses right now. The attacks are getting more targeted and more convincing. A single click on the wrong link can encrypt your entire network in minutes. Your defense has to be layered, monitored, and tested.

Hardware Failure

Servers fail. Hard drives fail. The question is whether you find out proactively or after the fact. Good server hardware with active maintenance contracts means you can get certified replacement parts quickly. Good monitoring of server storage catches predictive failure alarms before a drive actually dies — that's a proactive support case, not a disaster.



LATTIS

Extended Power Outage

Not a 20-minute blip. A multi-hour or multi-day outage takes down everything that isn't on generator or redundant power. Battery backups buy you time. They don't replace power. If your business can't survive eight hours without electricity, you need a plan for that.

Internet Outage

A fiber cut on the street can take your ISP down for hours. If your business depends on the internet — cloud applications, VoIP, email, payment processing — you need a backup ISP. Cellular failover works. A secondary wired connection works. Hope doesn't.

Phone System Failure

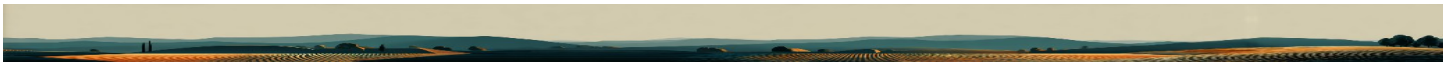
An old PBX dying is a special kind of painful because the parts often don't exist anymore. We've moved clients to GoTo cloud phone service in an afternoon — voicemail, call routing, automated attendants, and softphones on laptops and cell phones while the desk phones ship. Cloud PBX is now the right answer for most businesses.

If You Don't Have a Plan, You're at the Mercy of What's There

When something goes down and there's no DR plan, recovery is improvised. You work with whatever you have. If you have a functioning backup, you initiate a restore. If you're running a hypervisor — VMware, Hyper-V — that restore can be fast. If you're on a physical server, it takes longer. Much longer sometimes.

If you don't have a backup, or haven't tested it, recovery becomes a data recovery conversation. That's expensive, slow, and not always successful. The time to find out your backup wasn't working is not when you need it.

Know Your Numbers — Recovery Time and Recovery Point



LATTIS

Two questions every business owner needs to answer before choosing a backup and recovery plan:

First: How long can you be down? An hour? Four hours? A full day? A manufacturer running a production line has a very different answer than a winery between harvest seasons. Your answer determines what kind of recovery plan you need and how much it's worth spending. If you can't afford more than two hours of downtime, your recovery plan needs to match that.

Second: How much data can you afford to lose? If your backup runs nightly and your server fails at 4pm, you've lost a full day of work. Is that acceptable? For some businesses yes. For others — an accounting firm mid-close, an ag operation during a critical window — the answer is no. More frequent backups cost more. But so does recreating a day's worth of transactions from paper records.

Know your answers before you build your plan. They drive every other decision.

Backups — The 3-2-1 Rule and Why Testing Matters

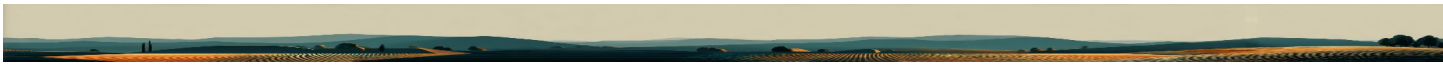
The 3-2-1 rule: three copies of your data, on two different types of media, with one copy offsite. This isn't optional — it's the baseline. If you don't have this, start here.

A backup you've never tested is not a backup. It's an assumption. Test restores regularly — at minimum quarterly. Know how long a full restore takes before you need to do one under pressure. If it takes 14 hours to restore your server and your business can't survive a day offline, that's a gap you need to close before the event, not during it.

Don't just check that the backup ran. Check that the data is actually there and restorable. Automated validation tools exist. Use them. A green checkmark in the backup console means the job completed. It doesn't mean the data is intact.

Data retention matters more than most people realize. Ransomware can sit dormant in your systems for weeks before it activates. If your retention window is 30 days and the malware was planted 45 days ago, every backup in your rotation is already compromised. Know your retention window and make sure it's long enough to reach back past a reasonable dormancy period.

Monitoring — Find Out Before It Becomes a Disaster



LATTIS

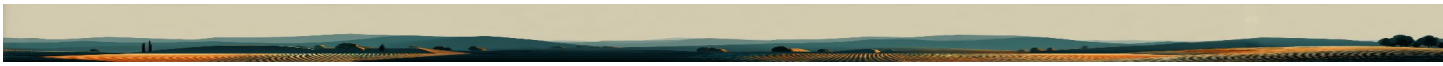
A properly managed monitoring system catches most hardware failures before they happen. A hard drive throwing predictive failure alarms is a support ticket, not a disaster — if someone is watching. A server running out of disk space is a five-minute fix — if someone notices before it causes an outage.

The difference between a managed network and an unmanaged one shows up most clearly in a crisis. Managed means someone already knows something is wrong before your staff reports it. Unmanaged means you find out when the phones stop working.

Vendor Contacts and SLA Documentation

When something fails at 2am, you need to know who to call. Not just your IT provider — your hardware vendor support line, your ISP, your phone carrier, your cloud service providers. Every critical system should have a documented support contact, account number, and SLA response time sitting somewhere outside the system that's down.

Most businesses don't have this. The information lives in someone's head, or in an email account they can't access because the server is down. A single printed document — or a copy stored somewhere offsite and offline — can save hours when hours matter most. Build it before you need it.



LATTIS

Who's in Charge When Things Go Wrong?

Every business needs a named person responsible for initiating disaster recovery. Not "IT" generically — a specific person with a specific role. When something goes down, everyone looks at each other. That costs time you don't have.

Document a simple call tree. Who gets called first? Who makes the decision to declare a disaster and initiate recovery? Who communicates with staff and customers while recovery is underway? It doesn't need to be elaborate. It needs to exist, and everyone needs to know where it is.

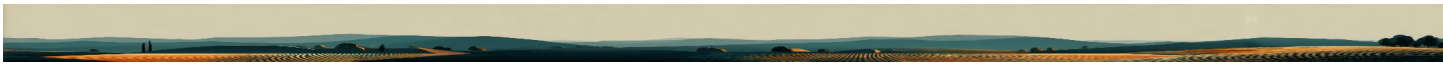
Physical Security — Don't Forget the Server Room

Disasters aren't always digital. A break-in, a theft, or unauthorized physical access to your server room is a disaster with the same consequences as a cyberattack. Who has access to your server room? Is it locked? Are you logging physical access? A camera on the door is a start. Access control is better. This connects directly to your overall security posture — physical and digital security are not separate problems.

Document Your Configuration — Before You Need to Rebuild

Most businesses have no written record of how their systems are configured. The firewall rules, the VLAN setup, the server roles, the application settings, the network addressing scheme. It all lives in the system itself — or in the head of whoever set it up. When that system is gone and you're rebuilding from scratch, the absence of documentation is not an inconvenience. It's a multiplier on your recovery time and your recovery cost.

I've seen rebuilds that should have taken two days take two weeks because nobody documented the configuration. Every setting had to be rediscovered, tested, and verified. In some cases the original integrator was gone and nobody knew what decisions had been made or why. Good documentation turns a rebuild into a recipe. Bad documentation turns it into an archaeology project.



LATTIS

At minimum, document your network addressing scheme, your firewall and switch configuration, your server roles and installed applications, your backup configuration, and your cloud service accounts and licenses. Keep a copy offsite and offline. Update it when things change. This is one of the most valuable things an IT provider can do for you — and one of the clearest signs of whether your current provider is managing your environment or just reacting to it.

Cyber Insurance — You Need It

Cyber insurance is no longer optional for businesses that depend on their systems. Carriers have raised the bar significantly on what they require before they'll issue a policy — MFA, verified backups, endpoint protection, no end-of-life operating systems. The questionnaires they send are detailed and technical.

Password Hygiene and Social Engineering — The Human Layer

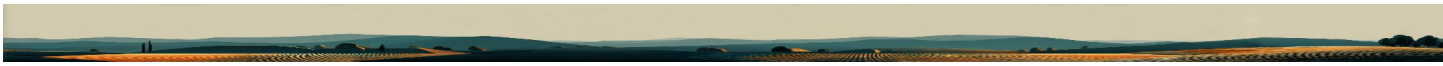
Good password hygiene starts with a secure password manager and two-factor authentication on every account that supports it. This is not optional anymore. Reused passwords are the single easiest way into your systems. A password manager eliminates the problem.

Social engineering — phishing emails, fake invoices, impersonation calls — targets people, not systems. Train your staff. Make it part of onboarding. When in doubt, pick up the phone and call the person directly. Don't reply to the email. Don't click the link.

Annual staff training is the minimum. The technical controls only work if the people using them know what to watch for. One hour a year is not too much to ask. The businesses that skip it are the ones that end up calling us after a breach.

⚠ WARNING: The Bank Account Switch Scam

Do not — under any circumstances — act on an email telling you that an owner, customer, vendor, or employee has changed their bank and wants you to update their wire transfer or direct deposit



LATTIS

information. This is one of the most common and most expensive scams targeting businesses today. The email looks real. It may come from a compromised account you recognize. Always verify by phone — not by replying to the email, not by calling a number in the email. Call the number you already have on file. Always.

Run a Tabletop Exercise

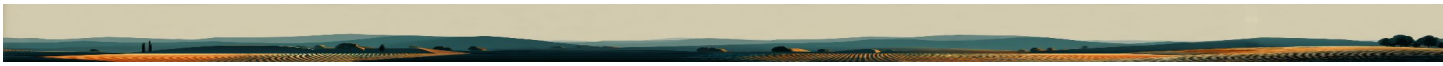
Large enterprises run formal disaster simulations. You don't need that. Once a year, sit down with your key people and walk through a scenario. "Our server failed this morning and we have no access to our files. What do we do? Who do we call? How long before we're back up?" Walk through it out loud, step by step.

You will find gaps you didn't know existed. A vendor number nobody has. A backup nobody has tested. A recovery procedure that lives only in the head of the person who's on vacation. A tabletop exercise costs an afternoon. Finding those gaps during a real disaster costs much more.

What a Real DR Plan Includes

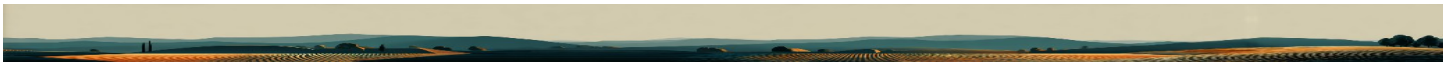
If you can check every item on this list, you're ahead of most businesses your size. Each unchecked item is a gap worth closing.

- ✓ **Documented recovery time target —** know how long you can afford to be down
- ✓ **Documented recovery point target —** know how much data loss is acceptable
- ✓ **Documented backup schedule —** with a verified retention window
- ✓ **Tested restore process —** you've actually done it, not just assumed it works
- ✓ **3-2-1 backup rule in place —** three copies, two media types, one offsite
- ✓ **Offsite or cloud backup copy —** physically separate from your primary systems
- ✓ **Redundant internet connection —** cellular failover or secondary wired ISP



LATTIS

- ✓ **UPS on all network gear and servers —** with batteries that aren't expired
- ✓ **Active hardware maintenance contracts —** on critical servers for rapid part replacement
- ✓ **Monitored storage —** with predictive failure alerting before a drive dies
- ✓ **Cloud phone system or failover plan —** documented and tested
- ✓ **Cyber insurance policy —** with current controls validated
- ✓ **Staff training on phishing and social engineering —** at least annually
- ✓ **Documented vendor contacts and SLAs —** stored offline where you can reach them
- ✓ **Named point of contact and written call tree —** for disaster response
- ✓ **Physical access controls —** on server room and critical hardware
- ✓ **Network and system configuration documented —** firewall rules, switch config, server roles, application settings, network addressing — stored offsite
- ✓ **Annual tabletop exercise —** walk through a scenario before it happens
- ✓ **Written recovery procedures —** documented, not just in someone's head



LATTIS

Lattis can help you build a plan before you need one.

We've helped businesses across San Luis Obispo and Santa Barbara Counties assess their exposure and put real recovery plans in place. If you're not sure where you stand, start with a conversation. We'll tell you what we see and what we'd do about it.

lattisnetworks.com/contact | (805) 470-7666