Today’s Disaster Preparedness

Maintaining Uptime While Avoiding Downtime

Stop planning to recover business-critical systems after downtime. Start protecting them from failing in the first place. In this guide, you’ll learn about the most common disaster avoidance mistakes your company can make and how to keep them from happening.

XANTRION
CYBERSECURITY • IT SUPPORT

Catastrophe Can't Stop Commerce

In the hours immediately after San Francisco's 1906 earthquake, the city's major bankers sealed their cash and records in their vaults to protect them from the approaching fires. Only Amadeo Giannini, founder of the small local Bank of Italy, realized the true danger: the metal vaults would protect their contents, but they would remain too hot to open for weeks after the fires were out. Instead, Giannini spirited the contents of his bank's vault to his home outside the fire zone. While all his competitors were still cooling their heels, he opened a makeshift office in just days and returned to serving the devastated city. Thanks to his forethought, we know his business today as the nation's second largest bank holding company, Bank of America.

This bit of business history illustrates what small and midsize business executives already instinctively know: you can't stop disasters, natural or otherwise, but you can keep them from slowing your business down. Fortunately, disasters are rare, but that makes being ready for them even more important.

In the past, every organization needed a plan to bounce back if a disaster took down their business-critical systems. Today's technologies are designed to help your company maintain uptime instead of helping you recover after downtime. By embracing these technologies, you can help your company avoid these five common errors and be ready for the worst.

Today's technologies are designed to help your company maintain uptime instead of helping you recover after downtime.

Five Common Mistakes to Avoid

1–Exposing Critical Systems to Unnecessary Risk

If your office is wiped out by a storm, fire, or earthquake, will your applications, database, and backups vanish with it? If your business-critical systems are all on-premise, that's the risk you're running.

The latest cloud services make business continuity easier and more cost-effective than ever by enabling you to move most or all of your key infrastructure permanently out of harm's way. Even if you can't get to the office (or worse yet, no longer have an office to get to), the information and systems that keep your business functioning will still be available in the cloud from anywhere you and your employees have an Internet connection. If you use any of the small and shrinking number of line-of-business applications with no cloud equivalents, you can still reduce risk by moving them offsite to a secure, disaster-proofed co-location facility in an area with a lower risk of disaster.

2–Not Performing Due Diligence

What if the cloud vendor to whom you entrust your most important data has an outage, gets hacked, or loses its server farm in a flood? Moving systems to the cloud doesn't mean cloud vendors can't be impacted by issues of their own. Make sure the providers you choose have their own disaster preparedness strategies. Ask them to demonstrate their redundancy and failover setup. Ask them to provide a Service Level Agreement for uptime. Ask them for proof of regular testing. Ask them for audits of backups. And don't shift over your data or your responsibility for business continuity until you're satisfied with their answers.

3–Forgetting that Telephones are Infrastructure

If you're using an in-house system to manage your phone calls, losing your office means losing your phones, and with them one of your customers' main ways to communicate with you. Switch to a hosted VoIP company to ensure the equipment that actually runs your phone system is safely housed in a secure data center far from your office, with an easy way to relay your calls to an alternate number (a branch office, a mobile phone, a voice mail box) if necessary.

4–Failing to Perform Regular Backups

Putting your production data in the cloud or in a colocation facility ensures that your primary files are stored offsite, so they aren’t taken down by the same theft, failure, or disaster that affects your offices. However, putting your data in the cloud or a colocation should not be confused with backing up your information. Many cloud vendors will back up your data automatically as part of their own business continuity procedure, in case your most recent data gets corrupted or accidentally deleted. However, you may still want or need an additional backup to handle data that falls outside the vendor’s retention period, to protect confidential data, or to establish incontrovertible data ownership. Consider performing backups to a different cloud vendor or to an offsite service.

5–Indulging in Denial

The most dangerous mistake you can possibly make in business continuity is giving in to the temptation to think, “We don’t need to worry.” It doesn’t take a front-page catastrophe to wipe out your business-critical data. We’ve seen plenty of smaller disasters that led to complete server loss:

- A disgruntled ex-employee who stole servers and backups
- Smoke elsewhere in the building that set off sprinklers in the server room
- A poorly maintained HVAC system that made the server room overheat, leading to catastrophic hardware failure
- A lightning strike that fried electronics and corrupted stored data
- “Ransomware” that spread from a single infected computer to all the firm’s servers, encrypting all their data and making it completely inaccessible

The common denominators among all of them? On-premise IT infrastructure and staff who either didn’t realize there was a problem or didn’t have the time or resources to handle it. It could happen to you. In fact, it probably will at some point. But if you move to the cloud, your vendor will handle it for you, either by maintaining the cloud infrastructure for resilience and redundancy or by spotting and mitigating small issues before they interfere with IT performance.

By embracing the latest technologies, you can help your company avoid common errors that put data at risk.

Ready to learn more?
Get the latest news and IT tips from Xantrion.

Subscribe

XANTRION
CYBERSECURITY • IT SUPPORT

Xantrion
651 20th Street
Oakland, CA 94612

xantrion.com

(510) 272-4701