The Essential DR Cheat Sheet:

Top 10 pitfalls to avoid when re-inventing your disaster recovery program

cbts

Consult Build Transform Support

Every new malicious attack or weather catastrophe underscores the importance of reinventing your disaster recovery (DR) preparedness program.

More organizations acknowledge the reality of ever increasing threats to their business. For instance, surveys of more than 5,000 IT professionals worldwide in 2017 found that 47% of organizations suffered a failure that required the use of their disaster recovery technology. Furthermore, 46% of the respondents cited "ability to recover from disaster" as one of their most pressing concerns in 2018.

Among the organizations that reported losing data:

- 35% lost between a few minutes and an hour of data
- 28% lost a few hours of data
- 31% lost a day or more of data

(Source: "The 2018 State of Resilience," Syncsort and Vision Solutions)

Thus, the high risk of IT downtime—and the cost in lost revenue and reputation—creates a pressing need for certainty that DR programs deliver in a crisis. It's not enough to design a DR program you hope will work. You need to *know* it will work.

Delivering that kind of certainty often requires a reinvention of your existing DR program. The complexities of disaster recovery require a careful, well-thought-out approach to ensuring that resources are focused on the critical applications and infrastructure that drive your bottom line.

As you develop a more robust DR program, it's imperative to avoid the ten most common pitfalls we outline in this eBook from CBTS.

Pitfall 10: Not understanding the "five Rs" of DR

Success in DR flows from comprehensive planning that embraces five fundamentals:

1. Restoring systems. Hardware, virtual machines, containers, applications, and other aspects of your IT systems must be restored quickly and efficiently.

2. Resuming business functions. eCommerce, enterprise resource planning, and other vital operations must get back online as soon as possible.

3. Remediating data losses. Some data loss may be inevitable; your DR program needs to establish priorities, limit damages, and implement repairs.

4. Recovering primary resources. The most important IT resources must have the highest priority for recovery.

5. Returning home. Finally, your DR program must return IT operations to their "home" state.

The five Rs must work in unison—neglecting one threatens the effectiveness of the rest.

Pitfall 9: Lack of data classification and information lifecycle management to manage data footprint and value

All data is not created equal. Customer data that enables real-time business intelligence is probably far more valuable than archival data on supply-chain resources from five years ago.

Thus, it's imperative to classify data and to devise a system of information lifecycle management that helps establish priorities according to the data's footprint and value to the organization.

Data classification and lifecycle management require you to answer a few crucial questions:

- How fast is your data growing? If you're adding big-data or IoT systems that pump massive volumes of new data into your IT systems, then your DR program must account for that data growth.
- Which data has the highest business value? Prioritizing the most business-critical data helps shape the contours of your DR program.
- How does data value fold into your recovery goals? Disaster recovery planning has two pillars that guide program design:
  - Recovery time objectives (RTOs)—how soon you recover data
  - Recovery point objectives (RPOs)—how far back in time your data recovery goes

All these factors must be considered in the earliest stages of DR planning to avoid serious problems down the road.

Pitfall 8: Ignoring business functions that *should not* continue in a DR crisis operating model

If you're dealing with a cyberattack or regional weather catastrophe, some business processes have to wait until everything calms down. Because a crisis narrows your operating flexibility substantially, it's crucial to avoid expending limited DR resources on low-priority business processes.

Averting Pitfall 8 requires digging into all critical business processes and pulling in insights from across the organization. Top stakeholders have to agree on what must stay live and what can go on the back burner.

Your RTOs and RPOs will help you determine how long your company can survive downtime, and which processes will go the furthest toward protecting revenue, keeping people safe, and avoiding damage to your reputation.

The whole point of DR is protecting what matters most; you can't let low-priority processes get in the way.

Pitfall 7. No data integrity procedures

Data corruption is typically inevitable in sophisticated IT systems and complex organizations. It can be serious enough to trigger disastrous downtime, or it can pollute the process of creating backups and trying to restore them.

Whatever the cause of data corruption, your DR program must have procedures that maximize data integrity and anticipate the likelihood of corruption. Procedures might include copying tapes, backing up to the cloud, and error-testing your data. Hard disks should be scanned for sector errors that corrupt data. Repairs should not be put off.

One thing many IT teams have learned the hard way: It's crucial to avoid letting users into restored systems until you feel confident the data has been restored without corruption issues.

Pitfall 6: Underestimating the need for "crash consistency"

Restoring from a crash means spinning up several systems simultaneously. Thus, DR architecture must understand which applications and databases must be integrated, interdependent, and aligned when the time comes to restore.

Pushing for "crash consistency" means acknowledging that software dependencies require systems to come up in a specific order. You also need a point-in-time continuum that allows you to inform business users when applications are restored and safe to use.

Crash consistency is a nuanced challenge that can require substantial development expertise. If your IT team lacks experience in crash consistency, you should consult with an expert.

Pitfall 5: Treating DR as a silo instead of embracing as part of IT and business management

To work in a time of a critical incident, DR planning must be baked into the business processes of all key departments within an organization. That means consulting with your HR staff to identify people and roles in each department who will be accountable for DR.

Each division's data-availability requirements should inform your change-control process as you reinvent your DR program. Furthermore, you should implement user-acceptance testing (UAT) scripts to scan for oversights in program development.

Ultimately, securing stakeholder buy-in can make all the difference in DR. Everything you do to secure the participation of executives and division heads early in the process will pay dividends during the crucial design, implementation, and testing phases.

And if all goes well in those phases, you're in better shape to ensure a clean recovery if disaster strikes.

Pitfall 4. Failing to work with business users to prove connectivity and application function

The most difficult challenges of DR involve the resumption of business functions. You have to ensure business users can secure access to the sites they need. And you have to validate the integrity of applications and data during restoration or failover.

Fixing Pitfall 4 is an extension of Pitfall 5: Consulting with department heads and key technical people working for them to ensure they have a personal stake in the DR program. Reinventing your approach to DR will require extensive testing (see Pitfall 2) that will involve every key division of the organization. Tests may have to be conducted on weekends to avoid disruption, which requires another layer of cooperation with stakeholders.

These tests, which should happen more than once a year in most organizations, will be the venue for proving the efficacy of your DR efforts.

Pitfall 3. Lacking a documented return-to-normal outline

The DR priorities that sustain you in a crisis will not sustain the business once things start returning to normal. All the small-bore activities you shunted aside to keep the lights on will soon start piling up if you continue to neglect them—potentially triggering a new crisis.

To prevent that from happening, you need to create a documented outline directing the process of getting out of disaster mode and back into everyday operations mode. That means sitting down with top stakeholders and finding a consensus on the best way to restore regular operations. The written outline then instructs everybody what they need to do at each step of the process.

Departments will need to make people and resources available to you. Without a written outline to guide them, department heads will feel reluctant to help out because they can't anticipate the demands on their people and processes.

Pitfall 2: Failing to define DR test exercise requirements before architecting solutions

This is a subtle point lost in many organizations: DR programs must be rigorously tested in exercises that mirror a genuine emergency. Systems must be taken down and recovery sites must be brought up in real time to ensure everything flows smoothly and root out flaws in the system design.

In most businesses, the prospect of live secondary site testing is daunting. What if resources don't come back up as planned? How much disruption to business processes can the organization stand? Can exercises run on nights or weekends?

All these testing issues should be worked out before designing the DR solution architecture. Otherwise, you run the risk of building a solution that causes large-scale interruptions during the testing phase. If that happens, you undermine your DR efforts.

That support is crucial in every phase of DR.

Pitfall 1: Thinking you are staffed to handle a disaster alone

Even if you feel comfortable that you have the DR expertise on staff, how sure are you that they can perform in a crisis? Will they even be available? Essential personnel have an uncanny knack for being on vacation in remote backcountry locations when a crisis erupts at work.

Another point to consider: Are you insured for a crisis? If so, is that coverage substantial enough to sustain your business in an emergency?

As public, private and hybrid cloud platforms continue to evolve in capabilities new and very cost effective data protection solutions are available to companies of all sizes. What used to be beyond the reach of small and medium sized enterprise organizations is now on equal playing field because the cost of entry has become much more attainable.

A partner like CBTS can plug these gaps in your business continuity and disaster recovery programs. We can design, build, implement, document and test your DR environment to ensure you have the right DR solution for your exact needs. We also can manage and monitor your system 24x7x365 so you always have highly trained experts jumping into action at the first sign of trouble.

A well-managed crisis can be the defining moment that strengthens your organization for the challenges to come. Just make sure you mind the common pitfalls to reinventing business continuity and disaster recovery—and come to us for help if you need it.

About CBTS

CBTS is a wholly owned subsidiary of Cincinnati Bell (NYSE:CBB) that serves enterprise and midmarket clients in all industries across the United States and Canada. From Unified Communications to Cloud Services and beyond, CBTS combines deep technical expertise with a full suite of flexible technology solutions that drive business outcomes, improve operational efficiency, mitigate risk, and reduce costs for its clients.

Contact us today at 1.866.587.2287 | cbts.com