TeraGo

Agility . Reliability . Creativity

What's the Weakest Link in DR plans?

Canadian companies confess their shortcomings

An evaluation of Canadian organizations and their response to disaster recovery processes. A joint survey in partnership with IDC Canada.

IDC
Analyze the Future

What's the Weakest Link in DR plans?

Canadian companies confess their shortcomings

How do you know if your disaster recovery plan works? DR plans are only valid if they've been tested. IDC Canada found that 81% of Canadian businesses are not testing their DR plans to industry standards. An untested system is like playing Russian roulette with an organization's data. The impact of not having a robust DR program is that companies are at risk of not having any disaster recovery capabilities. Businesses don't know if their DR systems work, until they fail, and by that time it's too late.

From flooding that wipes out business operations for days to DDoS attacks that bring the entire Internet to a grinding halt, it's no secret that organizations have a need to have DR plan in place. To get a better understanding of this landscape, TeraGo partnered with IDC Canada to conduct a survey of Canadian businesses about their DR processes. Without a proper plan in place, organizations can bring upon them a host of issues that can cripple their business operations that will leave a lasting impact that can be hard to recover from.

When it comes to DR planning, the overall findings show that Canadian companies are inadequately prepared when it comes to disaster recovery. 45% admitted that they're unable to identify everything that could potentially jeopardize their organizations IT infrastructure and the data that's required to run their business. This report examines how businesses are impacted by DR and what means they need to take to avoid costly scenarios.

45%

admitted

that they're unable to identify everything that could potentially jeopardize their organizations IT infrastructure and the data that's required to run their business.

TeraGo

Agility . Reliability . Creativity

Deficiencies in Planning and Testing Remains a Big Issue

We all know that disaster recovery plans take time to develop and can be difficult to maintain. An effective plan must enable your organization to plan for disasters. This requires setting goals tied to hours for your recovery time objectives (RTOs) and recovery point objectives (RPOs).

A DR strategy needs to consider budgets, senior management's tolerance to risk and any regulatory obligations that your industry needs to adhere to. Availability of resources will come into play as you'll need to look at what are the technology and human constraints that could impact your plan being effective.

Establishing these objectives is critical if one is to know what steps to exactly take in a disaster scenario. ISO/IEC 27031, the global standard for IT disaster recovery states that, "Strategies should define the approaches to implement the required resilience so that the principles of incident prevention, detection, response, recovery and restoration are put in place." Your strategy is an overview of how you'll approach DR for your business and the plans you develop will describe how you do it.

Furthermore, without proper DR testing, hitting your RTO and RPO is like trying to shoot a target in the dark. Testing and validation of a DR plan should take place every quarter. This ensures that if there are any shortcomings in your testing plan, they can be quickly remedied before you're faced with a real disaster. You may be surprised to learn that only 10% of Canadian businesses are committing to this schedule.

For all but the simplest of IT infrastructures, annual DR testing is not sufficient and leaves businesses at risk of losing mission-critical data and as much as $686,250 per hour of downtime[1].

The good news is that developing and testing an effective DR plan isn't as costly as one would think. Thanks to cloud service providers, DR can be reliably and professionally managed by teams who have the expertise required to ensure that your DR plans are capable of withstanding any disastrous situation.

The good news is that developing and testing an effective DR plan isn't as costly as one would think.

When Disaster Strikes, Are You Ready?

When the Halifax and Bank of Scotland (HBOS) was struck by a power outage, their primary datacenters went down. While they had backups stored on secondary and tertiary datacenters, failover did not take place and mission-critical applications did not resume functioning. This was surprising to some members of the IT team, as they had just turned the datacenters on to make sure that they worked.

However, many members of the IT team were not surprised, as they knew that the latest iterations of their mission-critical applications on the datacenters had not been tested against the backup environment, and that simply turning on their

[1] http://v1.aberdeen.com/launch/report/knowledge_brief/8882-KB-disaster-recovery-roulette.asp

VM was no guarantee of successful failover. Furthermore, the financial institution had never tested their DR plan using a power-outage scenario, so they were only able to guess at the time-to-remediation.

The Result: No services were provided for a full business day. This includes no ATMs, online, and over the counter transactions. The monetary loss for the day, while not insignificant, paled in comparison to the lost accounts due to reputational damaged, as HBOS was the only bank that had to close as a result of the power outage. Their world-class DR infrastructure was crippled by inadequate DR testing and planning and the organization's RTO and RPO were not met. Of the businesses surveyed, 54% acknowledged that they don't have completed documentation to fully support a process to recover damaged IT assets back to normal operation.

An Inevitable Disaster Happens When You Set and Forget

If the set-and-forget model renders even the best DR infrastructure useless, why is it so commonly used? Canadian businesses are forgetting to test their DR plan, 41% in total confessed that they have a plan in place, but testing isn't a priority.

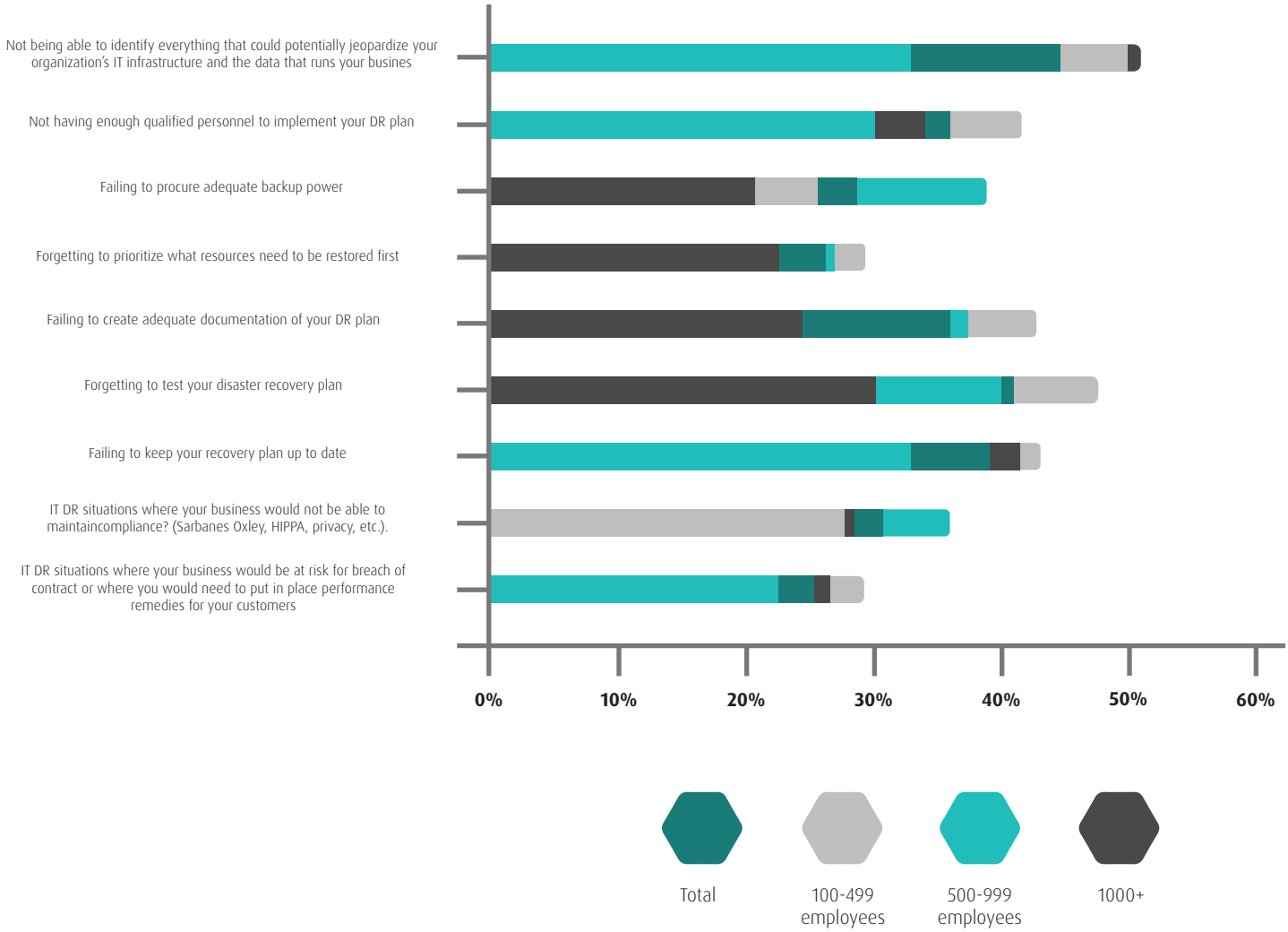
IDC Canada also identified that 45% of companies aren't able to identify everything that could potentially jeopardize an organization's IT infrastructure and the data that runs their business. Companies are under the assumption that they have a water-tight, disaster proof plan, but they're unaware of the plan's flaws unless they've seen it fail.

Furthermore, 36% of businesses made the admission that they don't have enough qualified staff to implement a DR plan successfully. There is an awareness that DR planning and testing is essential to their IT infrastructure, but there is a lack of expertise to successfully implement a plan. DR planning can be easily incorporated together with other IT processes and training activities, the ISO 27031 Section 7.5 states, "A coordinated program should be implemented to ensure that processes are in place to regularly promote DR awareness in general, as well as assess and enhance competency of all relevant personnel key to the successful implementation of DR activities."

The reality is that most in-house IT teams are swamped with day-to-day operations and rarely, if ever, manage to meet the DR planning and testing goals they initially set.

Top Confessions of DR Plan Weaknesses

- Not being able to identify everything that could potentially jeopardize your organization's IT infrastructure and the data that runs your business
- Forgetting to test your disaster recovery plan
- Failing to keep your recovery plan up to date
- Failing to create adequate documentation of your DR plan
- Not having enough qualified personnel to implement your DR plan



Lack of Resources and Understanding of Effective DR Planning

The reality is that most in-house IT teams are swamped with day-to-day operations and rarely, if ever, manage to meet the DR planning and testing goals they initially set out. Lack of resources, time and training explains why some companies neglect testing on a regular basis. Assessment and validation of DR tests can be a challenge if teams are feeling the crunch with other priorities.

Another underlying cause of failed DR planning is an inadequate understanding of what effective DR planning looks like. Of the businesses surveyed, 47% don't have a fully detailed and documented step-by-step process for an initial response to an IT disaster event.

Many IT managers aren't aware that it is their responsibility to test their DR after the initial DR system is set-up. Those that are often are not aware of how to properly test it. Many IT managers and CIOs buy DR solutions as a form of insurance. However, unlike insurance, DR infrastructure requires testing and maintenance. This is because, every time new applications and application updates are implemented, the DR system requires testing.

This was the problem in the case given with the HBOS. The old DR environment didn't kick in because it had not been tested with the most current applications. Just because you have a DR system in place, doesn't mean you have a fully optimized DR plan.

What A Sophisticated, Managed DR Solution Looks Like

As stated above, a DR implementation requires regular testing to ensure that the latest versions of your applications will function in the DR environment. This is not simply a matter of making sure your VM turns on. Each individual application needs to be tested to ensure failover occurs, and it is crucial to test after significant updates are applied. Having an exercise in a simulated recovery could prove beneficial. Only 52% of companies mentioned that they always perform operational tests to verify their recoverability metrics. If the financial institution from the case study discussed earlier had performed adequate testing, they would have known what their time-to-remediation would be and could have alerted their customers immediately, who then would have been able to plan accordingly rather than panic and potentially move their accounts to another institution.

DR implementation requires regular testing to ensure that the latest versions of your applications will function in the DR environment.

Proper Documentation Critical for RTO and RPO

To meet RTO and RPO, proper documentation is critical. Time-to-remediation must be recorded during testing for each application and process. This enables your IT department to take the steps necessary to optimize the DR system to hit its objectives. DR testing involves knowing how to properly measure and report the findings of the test and the best practices for conducting an efficient remediation.

Another key component of DR testing and optimization is that it requires that the entire DR environment be examined its processes prioritized. It's about understanding the best practices for testing each of your applications within various infrastructures, whether they be web-based, on-premises, or legacy. When the DR environment is not taken into account as a whole, processes can go awry quickly. This occurred with a crude oil trading company in Calgary, Alberta, during the 2013 flooding. Their online trading system that relied on a web client in the cloud, as well as on-premises datacenters. Their cloud service provider had made changes to their infrastructure, which the company had adjusted to months ago. However, they had failed to test their DR plan with the cloud infrastructure changes, and as a result were unable to meet their RTO when the flood struck.

Only 52% of companies mentioned that they always perform operational tests to verify their recoverability metrics.

Outsourcing is a Tantalizing Option

While being aware of what it takes to create and implement a successful DR testing plan is crucial to a successful disaster recovery, it also highlights the need for IT resources required for testing and implementation. While this can be done in-house, most organizations simply do not have the IT personnel necessary to maintain a reliable DR system.

This is where managed service and hosting providers come in. While your IT department's core competencies are in high-level areas such as application development and innovation, an experienced hosting provider will be able to take care of all DR implementation, management, and testing needs. Having a hosting

provider work closely with your team will ensure that nothing that could impede business functioning during a disaster would get overlooked. Large providers will be kept updated on best-practices for documentation and scheduling DR testing plans, and will have no shortage of staff to ensure that your DR infrastructure remains optimized for any scenario.

How a Hybrid Cloud Solution Can Help

One of the most effective but underutilized tools for DR is cloud technology. While many hard assets may need to stay on premise, enterprises can benefit from migrating soft assets to a stable cloud network. "Total cost of ownership (TCO) analyses have found that labour and staffing costs can be reduced by 40%-50% by leveraging the cloud," says Tony Ciciretto, President & CEO, TeraGo.

A migration to the cloud has the added benefit of ensuring that your data lives on a stable network. While your datacenter is subject to the elements, cloud infrastructure consists of multiple servers in various locations, providing reliable uptimes regardless of what happens in your neck of the woods. Had the financial institution described earlier used the cloud as part of their DR implementation they would likely have had at least partial access to mission-critical applications and would have been able to decrease their time-to-remediation for certain services.

Is Disaster Simulation the Answer?

Failure in having robust DR plans can be tied back to lack of senior management support and company culture. Disaster recovery is often an overlooked process. IT managers and CIOs need to be absolutely clear about the seriousness of potential risks that can halt a company's operations for days and weeks on end.

One way to convince them is to carry out a DR simulation test. This exercise would involve simulating an actual disaster. Use all the equipment, supplies at your disposal needed to create a real-life scenario.

Have business partners, employees and vendors participate in the process from start to finish. Document your findings and illicit feedback from them so that they can start buying into the concept of DR. The purpose of this test is to understand if you're able to carry out critical business applications during the event. The survey found that 46% of Canadian companies don't always identify and document their existing DR procedures.

The survey found that 46% of Canadian companies don't always identify and document their existing DR procedures.

Get Serious About Your DR Planning

DR is only underfunded due to misunderstandings concerning what an effective DR plan looks like. Every organization has different needs and there is often a lack of available in-house IT personnel to effectively design and test a DR system. A solution can be as simple as outsourcing DR planning and testing to a reliable company and will help ensure your DR system is effective in the event of a disaster.

TeraGo
Agility . Reliability . Creativity

7 Steps to Having a Best-in-Class DR Plan

Here's everything you need to successfully recover

Step 1: First run a risk assessment and a business impact analysis (BIA) to get a better understanding of what IT services are necessary to support your company's critical business activities.

Step 2: Define your RTOs and RPOs for all critical applications. Is there an acceptable amount of downtime that is tolerable in the event of a disaster or outage?

Step 3: Develop an easy-to-use repeatable process that covers off each step for recovering damaged IT assets and the procedures involved to have them return back to their normal operation as soon as possible.

Step 4: Simulate a disaster and plan for all contingencies (i.e. natural disaster, security breach). Includes training relevant staff members as to the processes and procedures in disaster recovery scenarios; who does what, when, and how.

Step 5: Identify key infrastructure and assess gaps, especially for mission-critical applications and prioritize their failover. Plan for duplication of critical skills, so that there is at least one back up person who can document procedures and pass on the retention of knowledge.

Step 6: Define your policies and test frequently, whether that's at your site, off site or with a vendor that can validate all of your DR procedures.

Step 7: Document time-to-remediation for all elements of your IT infrastructure so that the potential impact of downtime can be mitigated at all times.

The weakest link in a DR plan is that companies are unable to categorize all of the components necessary to make a DR plan successful. Best practices should have more detailed plans in place which clearly identify the critical applications and vital components required for a positive outcome.

More prepared organizations understand the importance of setting metrics that are tied to RTOs and RPOs. Defining all components at the start is critical for a plan's success and testing will inevitably fail if there isn't a solid plan in place to begin with. Be persistent with your DR planning — it will eventually pay off. Organizations that make the necessary investment in proper planning and testing will be the real winners when disaster strikes.

40%
of businesses do not recover
after experiencing a major disaster.

Source: FEMA

About TeraGo

TeraGo as a cloud service provider, offers a range of IT infrastructure services. We often engage with customers who contact us at critical times when their IT infrastructure has been impacted. After multiple of these occurrences, we recognized that the scope of the issue is wide spread, and the impact isn't fully appreciated within the business community.

We engaged in a joint study between TeraGo and IDC that surveyed over 200 businesses across all verticals and company sizes. The study revealed that most Canadian businesses are not adequately prepared when it comes to IT disaster recovery. Businesses either do not have a DR plan in place and even if they do, those plans are not regularly tested. Most companies are lacking the skills and resources required to have a robust, regularly tested DR plan.

As a Premier Canadian Partner in the VMware Service Provider Program, TeraGo is part of the vCloud Air Network. Through this strategic relationship with VMware, TeraGo gives enterprises better options to manage their hybrid IT platforms, while providing them the power to build, scale, and operate cloud services that maximize business opportunities.

vmware®

vCloud Air™ **Network**