CanadianCIO

What You Need to Know to Create a Modern Disaster Recovery Plan for the Cloud

SPONSORED BY:

TeraGo

IT executives have a lot to worry about these days. According to the *Canadian CIO Census 2017*, uptime and disaster recovery rank high on that list. It's no wonder. In an era where your customers expect "always on" service, you can't afford downtime. Worse still, 60 per cent of companies that lose their data will shut down within six months of a disaster.

Yet many companies admit they're not prepared for a disaster. Forty-five per cent say that they can't identify everything that could jeopardize their organizations.

At the same time, IT teams are under pressure to deliver transformation and increased agility for their organizations. The reality is that, on a day-to-day basis, they get stuck in reactive mode protecting against mistakes and malice, and getting bogged down in backups and cloud complexity.

What if you could keep your data safe and focus on innovation?

This can be achieved with a comprehensive IT resilience strategy for the cloud.

"You could do a consolidation or a systems upgrade and the disruption might be as bad as a natural disaster."

– Dmitri Li, Systems Engineer, Zerto

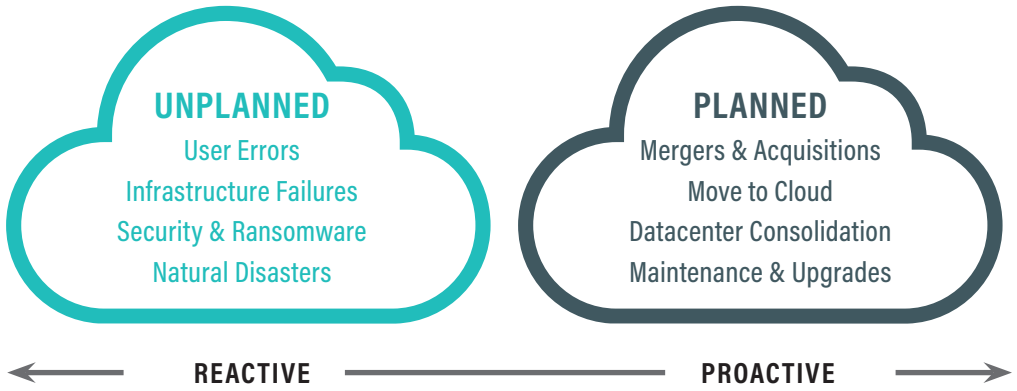
IT resilience is the ability to accelerate digital transformation and innovation by adapting to change while protecting your business from disruptions of any kind.

Here is what you need to know to develop a solid resilience plan, along with practical steps to implement it effectively.

PREPARE FOR PLANNED AND UNPLANNED EVENTS

IT resilience is about more than preparing for disasters. Organizations need to be ready for the potential impact of both planned and unplanned events, says Dmitri Li, systems engineer with Zerto. "You could do a consolidation or a systems upgrade, and the disruption might be as bad as a natural disaster," he says. "The idea of IT resilience is to keep you safe in either case."

Organizations need to shift from a reactive mode of operations to a proactive one, says Li. "With a resilient-first mindset, the protection comes along with you as you evolve your operations and business."



THE THREE PILLARS OF IT CLOUD RESILIENCE

A thorough resilience strategy should include the following key elements:

CONTINUOUS AVAILABILITY

- Outages & Disruptions
- Ransomware Attacks
- Complete Data Protection

WORKLOAD MOBILITY

- Infrastructure Modernization
- Consolidations & Migrations
- Testing & DevOps

MULTI-CLOUD AGILITY

- Cloud Integration & Migration
- Multi-Cloud Hybrid Cloud
- Analytics Across Clouds

First, the platform should deliver continuous availability for an always-on customer experience, backed by solid service-level objectives. The new generation of resilience platforms replaces multiple legacy solutions by using virtual replication to automate recovery from site failures, application failures across virtual machines, or a single virtual machine failure. Everything is captured so an organization never has to worry about large gaps of data loss when recovering.

Li says the concept is similar to a DVR used to record your favorite television programs. "Imagine being able to rewind things to a certain point in time before a disaster," said Li. Other approaches like daily backups or storage replication can result in some data loss and involve delays to recover the data. With the new, proactive approach, it can be recovered in 15 minutes or less, which could save "hundreds of thousands of dollars in the event of just one disaster," says Li.

Secondly, the platform should allow for workload mobility to easily move applications and workloads without risk. Whether it's part of a broader transformation or a consolidation, organizations need confidence that it will be safe to move workloads.

Thirdly, it should include "multi-cloud agility," allowing moves to, from or between clouds to meet application requirements and to control costs.

The ability to move workloads or applications may be the most important element, says Li. "Making your workload mobile enough that it can go to, from or between anything will reinforce your continuous availability. If something happens at data centre A, you can easily spin it up at data centre B or in the cloud."

WHY BACKING UP IS NOT ENOUGH

Many disaster recovery strategies focus primarily on backing up an organization's data. However, there are limitations to this approach. In most cases, backups are done on a daily or 24-hour basis during off-hours. This means a failure could result in a data loss of up to 24 hours. As well, it could take 24 hours or more to recover the data, impacting the desired RTO (recovery time objective) and, ultimately, the business.

While storage replication can reduce the impact, there are limits on how often you can take data snapshots, and it may still take a few hours to recover the data. As with backups, snapshots create a point-in-time record, and will always result in an RPO (recovery point objective) gap.

With virtual replication, the recovery point will be under 20 seconds, and it will take 15 minutes or less to recover the data. If, for example, there is a ransomware infection that occurred two hours ago, the company will not suffer the data loss going to the last backup. Instead, it will be able to rewind and recover to just seconds before the infection occurred.

FIVE PRACTICAL STEPS TO MAKING SURE YOUR CLOUD DISASTER RECOVERY PLAN WORKS

1. ASSESSMENT

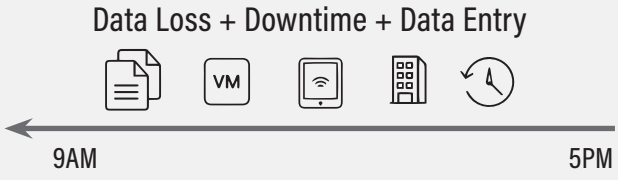
The first stage, the assessment, is critical to developing the business case for executives, says Mohamed Jivraj, TeraGo product manager.

A resilience assessment should be conducted to review the technology environment. Workloads and applications should be identified and priorities established in terms of the order in which VMs (virtual machines) need to be up and running. Service-level objectives (RPOs and RTOs) should be determined for the workloads. This evaluation results in a detailed assessment report.

A detailed cost analysis should be completed during this phase. It should include estimates of the cost of downtime (see below) and compare the costs of using a service provider to manage the platform versus doing it themselves. Typically, IT teams spend 75 per cent of their time managing operations and disaster recovery. As such, Jivraj says there may be significant savings to have a service provider support your disaster recovery plan.

BUSINESS IMPACT OF ONE/A SINGLE DISASTER

RPO 24 Hours		RTO 24 Hours	Impact $821,917
Storage Replication	RPO 4 Hours	RTO 4	Hours Impact $136,986
Zerto Virtual Replication	RPO 20 Seconds	RTO 15 Minutes	Impact $2,980



Minimize impact, rewind and recover anything in minutes, from any point in time, direct to production or recovery site

With this information, the organization should consider cost constraints and carefully determine the right level of resilience for different parts of the business, striking a balance between investment and risk tolerance, says Jivraj.

2. PLATFORM DESIGN

The planning stage includes the development of the technical design and the procedures to support the disaster recovery plan.

With the increase of hybrid and multi-cloud solutions, organizations need to work closely with their providers to ensure workloads and applications are in the right environment to meet the required service levels. As well, consistent with the pillars of IT resilience, they should make sure they can move workloads between clouds or to an on-premises location.

A "runbook" to outline all of the procedures for a disaster recovery plan is fundamental to its success. Yet, the IDC survey showed that 47 per cent of organizations don't have a fully detailed and documented step-by-step process for an initial response to an IT disaster event. The global standard for IT disaster recovery, ISO/IEC 27031, 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."

The runbook should include a detailed roadmap to outline the recovery objectives, authorizations, configurations, and failover and failback instructions.

A solid and up-to-date set of procedures provides calm and clear directions to help an organization resolve an issue, especially in a highly stressful situation.

CALCULATE THE COST OF DOWNTIME

Do you know how much an outage could cost your business?

Executives need to understand the costs of services not being available because "it's bigger than you think," says ITWC CIO Jim Love. "They need to have the details so they can have a conversation about it."

CLICK HERE to use a simple calculator to help you measure the business impact of an IT outage.

3. ONBOARDING

During this stage, the platform is implemented, and all of the procedures in the runbook should be finalized.

The first disaster recovery test should be done within 30 days after the onboarding is completed. Test results should be presented in a detailed report. "There's a level of confidence that you should get at the end of the onboarding period," says Jivraj.

4. MONITORING AND RECOVERY

IDC Canada found that 81 per cent of Canadian businesses are not testing their disaster recovery plans to industry standards. "An untested system is like playing Russian roulette with an organization's data," it says. Without proper testing, organizations will also stand little chance of hitting their recovery objectives.

Testing is an ongoing process. Organizations need to make sure the latest versions of their applications will function in a disaster recovery environment. After any updates are applied, it is crucial to test each individual application to ensure failover occurs.

"Things are so dynamic, you have to have a plan to test regularly," says Jivraj. "You need to be able to take all factors into account, and be ready to go in a heartbeat."

The IDC report notes that this also highlights the need for IT resources required for monitoring and testing. Organizations that do not have the IT personnel needed to maintain a reliable disaster recovery system may wish to consider outsourcing these functions to a service provider.

5. MAINTENANCE AND TESTING

Annual testing of the overall plan is not sufficient either. Rather, testing and validation should take place every quarter, so that any issues can be addressed before a real disaster occurs

"People underestimate the power of panic when a disaster happens," says Jivraj. "In the meantime, you need to be proactive to make sure your test plans are up to date, and that nothing has gone wrong with your disaster recovery." These functions can also be performed by a service provider.

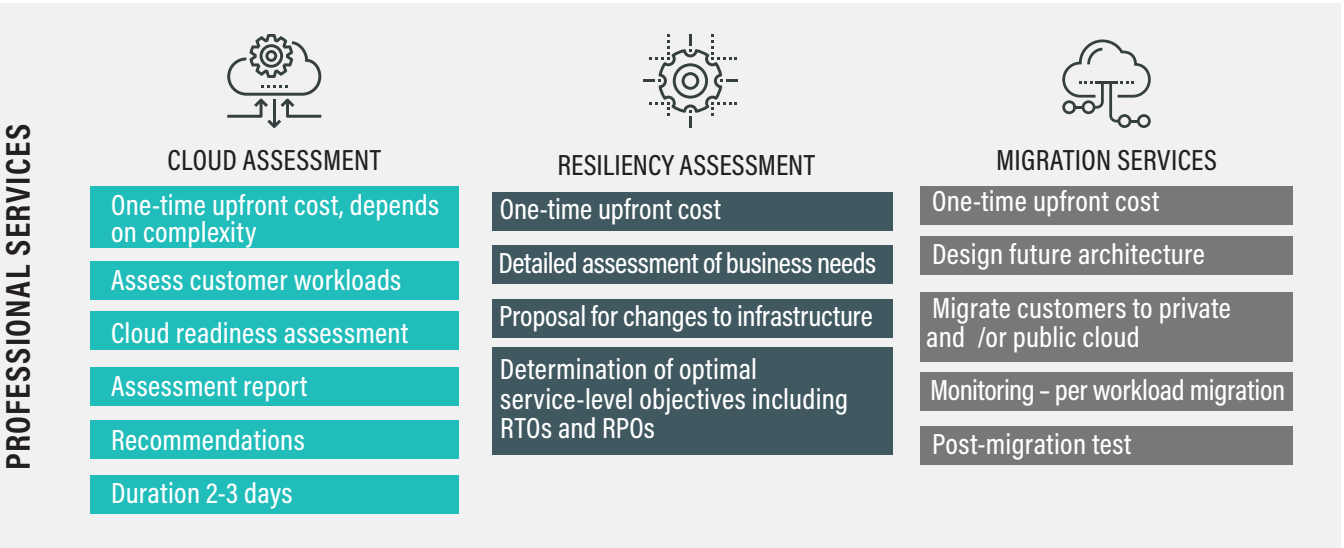
HOW TO CHOOSE A CLOUD SERVICE PROVIDER

Organizations should carefully evaluate available cloud service providers, based on the following six criteria:

- Is it a similar size company to yours? "You're looking for a consultative partner that is going to understand your needs because they are similar to their own," says Jivraj.
- Can it provide a one-stop shop in terms of a national network for connectivity, a data centre for colocation, private and public clouds and AWS solutions? Organizations need a service provider that can provide the right service for your workloads, simplify the architecture, and be the "go-to" for any issues.
- Can it offer expertise in a broad range of managed services? Disaster recovery is complex, and labour intensive. Make sure there is help available in case you need it.
- Does it specialize in disaster recovery and backup "as-a-service?" Ask about its disaster recovery expertise, and whether it has multiple data centres in different regions.
- Does it have experience in managing the overwhelming list of AWS services? Cloud service providers are an important part of the ecosystem, and can help sort through and manage the options.
- Does it have a national presence so that it can support data residency requirements. "Working with a service provider that can provide you with the sense that all of your confidential information is not leaving the county adds to your peace of mind," says Jivraj.

PROFESSIONAL AND MANAGED SERVICES TO CONSIDER

As organizations try to cope with the dizzying pace of technological change, many say they are looking for ways to focus on their core business. Some companies have delayed a move to the cloud because they don't have the technology or personnel to migrate their services without it having an impact on their day-to-day business operations.



This is where professional services, typically one-time engagements, can help an organization move forward. Many service providers offer these types of professional services.

Managed services, on the other hand, are more involved. This is where a service provider will keep tabs on an organization's environment on a regular basis. For example, managed security patching will ensure all aspects of a company's infrastructure, from hardware to the application level, is maintained and patched. Most companies find it difficult to keep up with patching, but it is a vital function to protect their data from threats.

Managed services, such as the following, can free up IT staff to focus on core business functions and innovation.

CONCLUSION

The IDC survey demonstrates that many organizations are struggling to maintain comprehensive disaster recovery programs. Today's cloud environments are becoming increasingly complex, and IT staff members are under pressure to support day-to-day operations while trying to move forward with transformation.

Next-generation IT resilience platforms enable organizations to shift from a reactive mode of operations to a proactive one of continuous data protection. These platforms come with professional and managed services so that IT staff can focus on innovative projects. They make business and financial sense and, in short, take the worry out of disaster recovery.

For a free Resilience Assessment, call TeraGo at **1.866.837.2465** or email **info@terago.ca**

ABOUT TERAGO

TeraGo provides businesses across Canada with cloud, colocation and connectivity services. TeraGo manages over 3,000 cloud workloads, operates five data centres in the Greater Toronto Area, the Greater Vancouver Area, and Kelowna, and owns and manages its own IP network. The Company serves business customers in major markets across Canada including Toronto, Montreal, Calgary, Edmonton, Vancouver and Winnipeg. TeraGo Networks is a Competitive Local Exchange Carrier (CLEC) and was recognized by IDC as a Major Player in MarketScape Cloud Vendor Assessment. TeraGo Networks was also selected as one of Canada's Top Small and Medium Employers for 2017.

ABOUT ZERTO

Zerto helps customers accelerate IT transformation by eliminating the risk and complexity of modernization and cloud adoption. By replacing multiple legacy solutions with a single IT Resilience Platform, Zerto is changing the way disaster recovery, data protection and cloud are managed. With enterprise scale, Zerto's software platform delivers continuous availability for an always-on customer experience while simplifying workload mobility to protect, recover and move applications freely across hybrid and multi-clouds. Zerto is trusted by over 6,000 customers globally and is powering resilience offerings for Microsoft Azure, IBM Cloud, AWS, Sungard AS and more than 350 cloud services providers.

Sources:

i "CIO as Innovation and Transformation Leader", The Canadian CIO Census 2017, by ITWC, page 13.

ii Data Loss Statistics, Boston Computing, https://www.bostoncomputing.net/consultation/databackup/statistics/

iii What's the Weakest Link in DR Plans?, A joint survey in partnership with IDC Canada, 2016

iv Ibid

v Ibid

vi Ibid