ITWC The Content Experts

WEBINAR HIGHLIGHT REPORT

Four Keys to Smashing Success in the Cloud

BROUGHT TO YOU BY

itbusiness.ca

SPONSORED BY

TeraGo

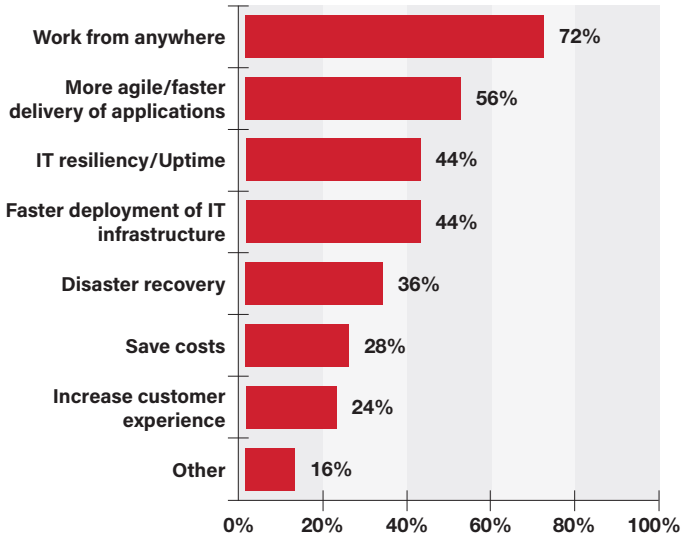
Most organizations move to the cloud for the cost savings, but adding other applications like disaster recovery to the mix is the way to truly capitalize on its value.

In ITWC's latest webinar, *Four Keys to Smashing Success in the Cloud*, Mohamed Jivraj and Nabeel Sherif of cloud provider TeraGo joined ITWC CIO Jim Love in a discussion about the cloud's place in protecting assets in case of disaster.

Business needs should drive your cloud strategy

Organizations are becoming more comfortable with the cloud, said Jivraj, a product manager at TeraGo. "There's a lot more confidence and faith in the cloud." Indeed, a poll of webinar attendees revealed that 36 per cent currently use disaster recovery (DR) in the cloud, and 44 per cent rely on cloud for resiliency and uptime.

POLL: Why are you using the cloud?



Respondents were permitted to choose more than one answer

"Moving to the cloud is always a journey," added Sherif, a TeraGo cloud specialist. "It's an evolution of how to use this new tool. The cost savings are there, depending on how well you execute. Most of the time, people don't really get the cost savings they expect in the dream state of cloud. But they achieve some cost savings and they find the flexibility to allow them to focus on real value generation and get away from the plumbing."

To achieve that value, Sherif said organizations need to tie results to a workload or a business process. They will have quick wins if the cloud improves operations. He cites four keys to success in the cloud as:

1. Disaster recovery
2. Security
3. Compliance
4. The right cloud mix

Resiliency in general – DR, backup, and other functions used on demand – are ideal applications for cloud, he said. "We've gone from a place where security and regulation were reasons to avoid moving to the cloud to a time when we realize that we often get better security execution by offloading the task to a cloud provider with the appropriate expertise."

Ultimately, cloud and data centre strategies will be driven by business considerations, as much as by technology and supplier choices, according to research firm IDC, "Adoption of best-in-class cloud models, as well as prevailing service-level agreements, security concerns, and financial optimization initiatives, will become ever more critical for the sustained success and performance of ICT environments — and business operations as well."

The industry is reflecting this change, with specialized companies popping up that focus on DR and business continuity in the cloud. Established vendors like AWS are also offering DR services.

Disaster recovery is a good place to start

DR is a way of moving sure-footedly into cloud, said Sherif. Cloud is about making applications work better and more reliably. One way to do that is making them resilient using DR.

"One of the biggest challenges in IT is what I call the janitorial work of running an IT system," he said." Work that's necessary, that's valuable to be done, but it's the kind of work where you're never going to get glory when it's done right, but you're certainly going to get a lot of trouble if you get it wrong." Patching and network optimization are examples of that kind of work. "If you can get away from doing these cumbersome, non-glory activities and concentrate your skill set and your team on actual value generation that's going to be appreciated, you're delivering better value to your business, and probably better satisfaction to your staff," he noted,

Sherif recommended that the so-called janitorial functions be offloaded to a competent cloud provider. In the first level of moving to the cloud, the provider handles basic functions like procurement and capacity planning, patching, security, hardware and software upgrades, mobility, accessibility and mobile device management, as well as simplifying the separation of environments for development, testing, staging, and production.

Jivraj added that many organizations struggle to implement DR or IT resiliency. It's important to start with the fundamentals, which involve business decisions, not necessarily technology, he said. First, organizations should define objectives, and determine that they match the desired business outcomes. For example, a decision needs to be made on which workloads should be restored first in case of disaster.

You also need to know how much data you can afford to lose and how much time you can afford to be idle, he explained. Organizations should also do a financial assessment on the business impact of an outage when deciding how much to spend on a DR solution.

The goal is to minimize the impact of an outage, so you also need to look at your provider's geographic portfolio, and contract accordingly, said Jivraj. For example, organizations need to look at putting the failover site in a different availability zone at a safe distance from the primary to ensure they both don't go down at once.

"When you're building out a DR solution, there are many key elements to designing a solution that will work," said Jivraj. Organizations first have to develop a plan, deciding on business priorities, risk tolerance, and other factors. Based on the plan, they should design a solution, then deploy it, monitor it to ensure it's performing properly, then maintain and test it, he said.

WHAT YOU NEED TO PROVE YOUR SUCCESS

PLAN
- Business priorities
- Risk tolerance vs risk – the right balance
- Defined RPOs and RTOs
- Identified resources
- Compliance needs

SOLUTION DESIGN
- System and network configuration
- Application details & dependencies
- Authorization & access details
- Roles & responsibilities
- Failover steps
- Escalation steps

DEPLOYMENT
Deploy solution design, system admin and operations for:
- DR software, virtualization technologies
- Storage, network and firewall configurations

MONITOR & RECOVER
- Monitor for scheduled replication tasks
- Ensure replication activities meet RPOs
- Fail-over (as per runbook) in case of disaster declaration and within predefined RTOs
- Complete failback once primary location is available

MAINTENANCE & TESTING
Maintain runbook:
- Quarterly; Capture updates required for software, infrastructure or personnel changes

Troubleshoot:
- Software and hardware components, including firewalls, DRaaS software and hypervisor layer

Test, test, test!

"People think they can just deploy DR and forget it," Jivraj said."You can't. A lot of changes happen on a daily basis. If you rely on a DR plan that's a year or even a month old, it risks a lot of your investment."

The focus should be on IT resiliency and business continuity, Jivraj said. It's not just about natural disasters. It can be about a power outage or human error too. Businesses should be more thorough about what happens if they can't access their environments and how much that would cost. TeraGo has an online tool to help people calculate the cost of downtime to help them decide whether to turn to a professional or handle DR in-house.

BUSINESS IMPACT OF 1 DISASTER

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

Data Loss + Downtime + Data Entry

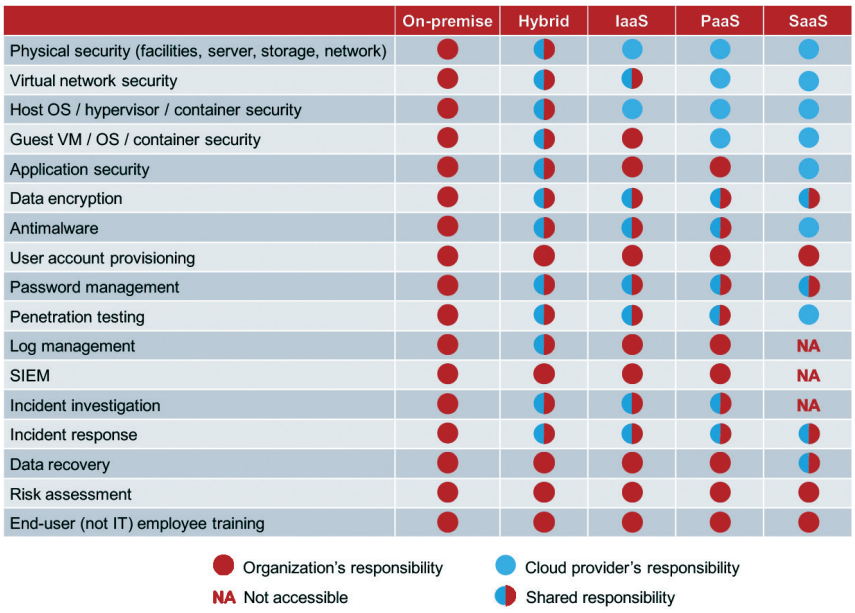
Security is a shared responsibility

There's been an "about-face" on security in the cloud, said Sherif. People once looked on hosted services and cloud with suspicion, whereas now they think that a competent provider can do better job than a company whose core competency isn't running network and system operations. One proof point for cloud occurred in 2010 when the hacker group Anonymous started its distributed denial of service (DDoS) attacks. The only system it couldn't kill was AWS, which was focused on system availability and performance.

Security, even in the cloud, is a shared responsibility, however, noted Sherif. There's the security baked into its systems by the cloud provider, and then there's the customer responsibility. It's important to understand who is responsible for each security component of the particular service solution and for the customer to properly use the tools offered by its provider to secure its systems. After all, Sherif said, "if you don't lock your doors and arm the alarm system in your house, you won't be secure even with the best locks and the best alarm system."

Love added, "If the provider can't discuss the shared responsibility model, run far and fast! The time when you have a disaster is not the time to say 'I thought you were ...'"

SECURITY OF THE CLOUD



	On-premise	Hybrid	IaaS	PaaS	SaaS
Physical security (facilities, server, storage, network)	●	◐	○	○	○
Virtual network security	●	◐	◐	○	○
Host OS / hypervisor / container security	●	◐	○	○	○
Guest VM / OS / container security	●	◐	●	○	○
Application security	●	◐	●	●	○
Data encryption	●	◐	◐	◐	◐
Antimalware	●	◐	◐	◐	○
User account provisioning	●	●	●	●	●
Password management	●	◐	◐	◐	◐
Penetration testing	●	◐	◐	◐	○
Log management	●	◐	●	●	NA
SIEM	●	●	●	●	NA
Incident investigation	●	◐	◐	◐	NA
Incident response	●	◐	◐	◐	◐
Data recovery	●	●	●	●	◐
Risk assessment	●	●	●	●	●
End-user (not IT) employee training	●	●	●	●	●

● Organization's responsibility
NA Not accessible
○ Cloud provider's responsibility
◐ Shared responsibility

Sherif agreed. "Companies need a provider who can walk them through the 'gotchas'. A good cloud provider has the technology, the resources, and the methodology, and they're practicing regularly, so they can improve a business's security," he said.

Getting cloud expertise on compliance

Like security, regulations, such as GDPR, and PIPEDA, are adding even more complexity to the task of information management. "Do you want to spend your time on compliance when it's not your core business, or let an expert provider handle it," asked Jivraj. "Compliance is vast. With data sovereignty as a critical concern of many regulators, service providers should ensure your data remains where you put it. The old model of not needing to know where your data is in the cloud is not longer viable in many cases. You have to know precisely where it is to remain compliant."

"Dealing with breaches is a reality," Jivraj observed. "But there are nuances." For example, many think that GDPR is an EU regulation, but anyone who deals with the EU has to comply. Canada has its own similar regulation. There are regulations at the datacentre level and at the data level, as well as industry-specific regulations. "There are many companies who can help navigate all of them. It's worth the time to seek out a specialist," said Jivraj.

Choosing the right cloud mix

It's important to pick the right cloud mix because certain workloads perform best in different environments, said Sherif. "People often start by tossing a bunch of stuff into the cloud," he said. "Soon they start to realize they're not generating the savings or are not achieving expected performance, and re-examine the environment." Companies usually evolve to a model with different workloads and IT assets running in different environments. "The challenge is in deciding what goes where," said Sherif.

As a general rule, the need for elasticity and redundancy in an environment with demand spikes, volatility, and lack of internal skillsets, makes a workload a good public cloud candidate. A private cloud might be more suitable when there's predictable consumption, sufficient scale to justify running an environment, and when the cost and management effort to add capacity is cheaper than it would be in the public cloud.

A rule of thumb for disaster recovery is to choose the public cloud when recovery point and recovery time objectives (RTO/RPO) are greater than 24 hours, or when you're dealing with workloads that are usage based. Choose a private cloud when RTO/RPO is less than 24 hours, or when data sovereignty is a concern because some public clouds have only one datacentre in Canada. A caveat is that you need to have the skill set to manage it.

As people move to the cloud, they tend to start with one provider, but eventually realize that they shouldn't have put everything in one place. Sherif said Forrester Research has revealed that 56 per cent of organizations surveyed use multiple cloud solutions to improve security and compliance, data management, infrastructure management and flexibility. Smashing success in DR is about building a plan in a thoughtful holistic way and then executing on it.

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 its MarketScape Cloud Vendor Assessment. TeraGo Networks was also selected as one of Canada's Top Small and Medium Employers for 2017.

www.terago.ca

About ITBusiness and ITWC

ITBusiness.ca is published by ITWC, a privately-owned digital media and content services company. Building on more than three decades of solid relationships with Canada's technology decision-makers through award-winning excellence in journalism, ITWC delivers incisive, relevant information to executive and managerial audiences. It also provides leading, integrated marketing content strategies to clients, including more than 200 global Fortune 1000 companies.

ITWC is the exclusive Canadian affiliate of International Data Group (IDG) which publishes more than 300 publications worldwide.

www.itbusiness.ca | www.itwc.ca