THE INTELLIGENCE OF BUSINESS CONTINUITY MANAGEMENT; It's As Simple As 3-2-1!

Contents

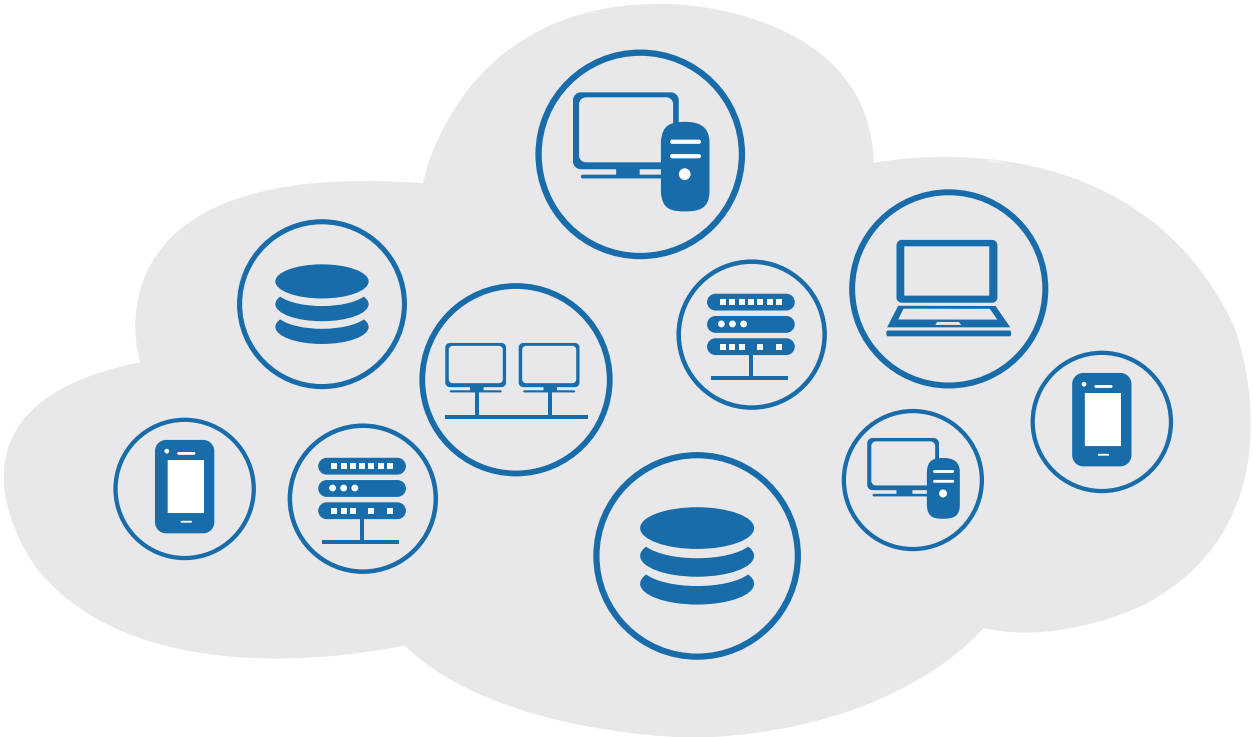
Executive Summary

Ensuring continued business operations before, during and after any disruption continues to be a challenge for enterprises of all sizes. Businesses are creating and storing more critical data both internally as well as in third party locations including public clouds.

Developing a Business Continuity Methodology (BCM) will ensure that IT can meet the recovery time (RTO) and Recovery Point Objectives (RPO) of users. Key elements must address how many and where back-up copies are stored, as well as solutions and partners that are best suited to support a **BCM** plan.

Consider using the "3-2-1" rule for back-ups: have three copies of your data, storing copies on two different media types, with one copy stored offsite.

Planning must also take into consideration a cultural and strategic fit around risk mitigation and its inherent value to operations and revenue.



INFORMATION EVERYWHERE, ALL THE TIME

Business continuity is not a new practice and IT professionals have worked to develop resilient architectures for centuries. So what has changed? Why is business continuity more critical today? Cloud, digital business and continuous application development have forced enterprise infrastructure to be built and deployed in minutes instead of weeks. Developers and business units have begun to dictate infrastructure availability requirements and IT now needs to become more agile to keep up the pace. This is acutely evident in the provisioning of back-up services. Enterprises of all shapes and sizes are rethinking their data backup and business continuity strategies while looking at service providers as extensions of internal IT.

According to Gartner, by 2018, the number of organizations using disaster recovery as a service will exceed the number of organizations using traditional, syndicated recovery services.

The influence of cloud delivery models is widespread in most organizations - even those with compliance and data privacy concerns. On-demand compute, storage and back-ups are becoming the norm rather than the exception.

The architectures that cloud enables are a mixed blessing - **they provide the business with tools to be nimble and increase revenue but exert pressure on IT to cut its provisioning times by 70%.**

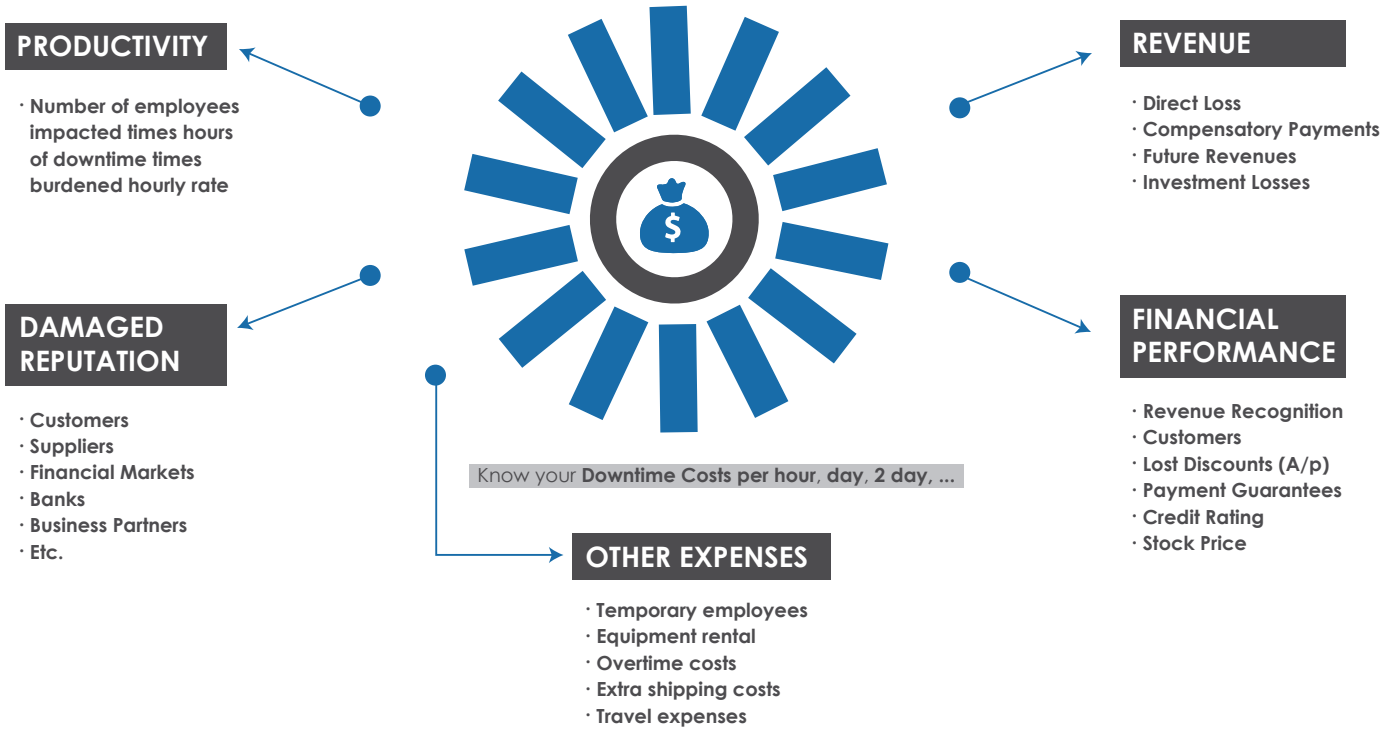
As more infrastructure is deployed for projects, critical business data becomes distributed across physical and virtual machines in both cloud and internal datacenters.

The hybrid IT or hybrid cloud environment promotes the on-demand provisioning of resources to meet a need, but many of hypervisor based workloads are not backed-up. As virtual machines are created, cloned, provisioned and deprovisioned, copies of data are dispersed all across the enterprise servers as well as the cloud. This lack of centralized storage and management of data is a huge risk for data privacy.

According to Gartner, nearly half of large enterprises will have hybrid cloud deployments by 2017

In addition to managing hybrid cloud environments, most users are expecting higher levels of availability for their applications, whether or not they are critical in nature. No longer can enterprises endure downtime for several hours and escape without consequences. The cost of downtime reaches far beyond just the finacial impact. But fear not-enterprises can begin to tame the negative effects of downtime by following the process below.

WHAT IS YOUR COST OF DOWNTIME?



KEY STEPS OF SUCCESSFUL BCM PLANS

Developing the right plan for your enterprise is all about understanding what to **recover/back-up**, determining when you need access and which provider or solution is best suited to your needs. The input required to construct the plan needs to involve all major stakeholders including **application**, **architecture**, **network**, **storage** and **compliance teams**.

Understanding which applications and work-loads are critical and intolerant of downtime, dependencies embedded in your information architecture and the ability for IT to manage highly available environments are critical.

Key steps include:

Assessments - Business impact, operational processes and financial planning

Staffing

Assess both the level of staffing as well as skillsets of those involved in both day to day operations and declaration of disaster and recovery procedures. Does the current staff have the skills to recover data to meet **RTO** and

RPO requirements? How often does training and professional development activities occur in order to keep skills current? **Does the current staff have the ability to react to issues 24 hours a day?** If current staffing levels don't support continuous availability, utilizing a third party provider is an attractive option.

Governance

Many enterprises have little to no programmatic structure around business continuity operations. The goal is to develop a set of collective decisions and guidance as to when to enact risk mitigation, response, recovery and restoration procedures. **Proper governance occurs not just after an outage or disaster occurs for post-mortem activities; working to mitigate risks and improve availability show maturity in a governance plan.**

Process

For effective business continuity, you need to plan and manage the response to crisis. Governance plans address the high level framework around roles and responsibilities, but how those actions are implemented falls to process. **Disaster response teams must initiate and follow a BCM process to ensure that recovery procedures are seamless and communication to both internal and external customers is consistent and frequent.**

Risk sensitivity

Frequently overlooked, a business's appetite for risk will ultimately decide if a BCM succeeds or fails. **As the markets for cloud services grow exponentially, not all enterprises are comfortable or trust third party cloud providers.** Certain vertical industries including healthcare, pharmaceutical, financial services and governments have developed their own competencies and assets to support high availability architectures. The thought of data moving to the cloud to be recovered and restored for some is untenable. Balance agility, cost and business culture before committing to using a cloud provider for BCM.

Architecture

A comprehensive review of all components involved in an entity's enterprise architecture as well as interdependencies among applications is crucial. **Best practice dictates that back-up copies of data should be stored offsite but will be rendered useless if your primary wide area network connections are down.** Identifying gaps in resiliency based on datacenter, server, storage and network capacity will help guide decisions around whether investments in capital or a shift to external resources make the most sense.

Budgeting

A true BCM plan is not funded in a reactive, ad hoc manner, but one built around an annual budget aligned with business and operational goals. Each aspect of the plan-back-up, disaster recovery, crisis management and testing are adequately funded and are measured by key performance indicators. Most BCM budgets will be stretched; **Gartner predicts that 64% enterprise recovery time objectives will fail within hours.** Enterprises in highly transaction dependent and compliant industries typically shoulder greater RTO burdens.

WHAT ELEMENTS SHOULD I RECOVER?

For most enterprises, target backup and recovery environments are primarily virtual machines with VMware, Hyper-V or Linux based hypervisors. Most enterprises have undergone shifts from physical to virtual servers and storage environments have seen the number of VMs grow dramatically. Consequently, backing up every VM will prove to be costly and labor intensive. Some of these VMs are created on premise and some are created in a cloud platform. Other platforms that must be considered for data availability include:

Bare metal instances

Bare metal continues play a significant role in cloud architectures. Their ability to recover and restore down to a fine grain level requires a specialized skillset.

Converged infrastructure

The emergence of converged infrastructure solutions from providers such as Nutanix and Simplivity require understanding of both these solutions' proprietary virtualization technologies as well as their ability to integrate with platforms such as VMware site recovery manager.

Dedicated infrastructure

Traditional dedicated and physical servers and storage also play a role for databases and other compute intensive applications. However, IT managers tend to only back-up and restore applications on dedicated servers to dedicated target environments. This can prove costly and inhibit flexibility when attempting to restore specific applications. It's crucial to understand if interdependencies exist between on premise and cloud infrastructures, as well any proprietary tasks involved with the software hosted by these dedicated infrastructures.

RTO AND RPO - HOW MUCH IS ENOUGH?

It's natural to want to protect and restore the most valuable assets of a business, but business continuity comes with both operational and capital costs that must align with the needs of the business and its customers. The process of identifying what systems and applications require immediate restoration and which can tolerate a degree of downtime is different for all companies. **However, certain industries rely on critical systems and require more aggressive time frames:**

EXAMPLE VERTICAL INDUSTRIES	RTO TARGET	RPO TARGET	AVAILABILITY TARGET	IT BUDGET ALLOCATION
Financial Services, Mission Critical Healtcare, Utilities	Between 0 and 2 hours	Between 0 and 2 hours	99.95 % or higher	7% or more
Manufacturing Pharmaceutical Professional Services	Between 0 and 8 hours	Between 0 and 4 hours	Between 99.7% and 99.94%	Between 3% and 7%
Higher Education, Consumer Goods, Government Agencies	Between 0 and 24 hours	Between 0 and 12 hours	Between 99% and 99.69%	Between 1% and 3%
Food and Beverage, Hospitality, Nonprofit	24 hours or greater	24 hours or greater	Less than 99%	Less than 1%

RTO = recovery time objectives, **RPO** = recovery point objectives

Source: Gartner (June 2015)

When determining your **BCM** strategy, involve all stakeholders as they often have transparency into areas you lack, such as downstream dependencies, financial impacts and operational ramifications. Once you have collected all the relevant business, operational and financial data for your enterprise, you can determine your own recovery time and recovery point objectives.

Recovery time objective (**RTO**) refer to the duration of time a service level within a business process must be restored after an outage of disaster is declared. **RTO metrics** are measured in windows of time ranging from less than 1 hour up to 48 hours. The higher cost of downtime to the business, the lower the **RTO** metric that is usually required. Recovery point objective (**RPO**) refers to the maximum allowable period that data might be lost due to an outage or disaster. The critical factor that determines **RPO** is the time between an enterprises' last data back-up and an outage. **RPO** windows can be managed with tighter data back-up and synchronization schedules, but orchestrating and managing that process can be complex and expensive.

Third party cloud back-up and recovery services offer the ability to manage synchronization to both private and public cloud resources as well as support both implementation and failover processes. Solutions like Veeams's availability suite supports speed recovery as well as visibility into production and target environments. Prior to engaging a cloud or hosting provider for business continuity services, determine your preferred **RTO** and **RPO metrics** and use those metrics to create meaningful and business centric service level agreements with your provider.

Conclusion

Becoming a business continuity hero is not an overnight process; it requires the ability to understand what's most important to your business and the foresight to ensure recovery times can be met.

Effective strategies emphasize both people and process. Employ the 3-2-1 availability strategy with three copies of data, storing copies on two different media types with one offsite as the foundation for BCM.

Enterprises that don't have the skillsets and staff must look at using third party providers that can deliver both cloud and on premise based BCM services, wrapped with service level agreements that both provide compensations as well as shared risk.

About PhoenixNAP

PhoenixNAP® is a global IT services provider offering progressive Infrastructure-as-a-Service solutions from locations worldwide. Bare metal server, cloud, hardware leasing, and colocation options are complemented with backup and recovery services, Disaster-Recovery-as-a-Service, and Managed Services to meet the evolving technology demands businesses require without sacrificing performance. Scalable OpEx solutions to support with the systems and staff to assist; phoenixNAP global IT services.
Visit www.phoenixnap.com and follow us on Twitter, Facebook, and Google+ for more information.

About Veeam Software

Veeam® recognizes the new challenges companies across the globe face in enabling the Always-On Enterprise™, a business that must operate 24/7/365. To address this, Veeam has pioneered a new market of *Availability for the Always-On Enterprise™* by helping organizations meet recovery time and point objectives (RTPO™) of less than 15 minutes for all applications and data, through a fundamentally new kind of solution that delivers high-speed recovery, data loss avoidance, verified protection, leveraged data and complete visibility. Veeam Availability Suite™, which includes Veeam Backup & Replication™, leverages virtualization, storage, and cloud technologies that enable the modern data center to help organizations save time, mitigate risks, and dramatically reduce capital and operational costs, while always supporting the current and future business goals of Veeam customers.

Founded in 2006, Veeam currently has 37,000 ProPartners and more than 183,000 customers worldwide. Veeam's global headquarters are located in Baar, Switzerland, and the company has offices throughout the world.
To learn more, visit https://www.veeam.com.