Ready for Resiliency?

KONICA MINOLTA | WEAPONS
IT SERVICES FROM KONICA MINOLTA

The Complete Guide to Disaster Recovery & Business Continuity

On average, companies lose **$84,000** for every **hour of downtime.**

Introduction

Data and productivity are the lifeblood of your business. Are you doing enough to protect those vital assets?

In this eBook, Canadian IT experts discuss the ins and outs of Disaster Recovery planning, business continuity, data backups, and business resiliency.

Disaster Recovery 101

Productivity is key to the success of any organization. As Canadian businesses grow and evolve, one important management discipline is often ignored… planning and strategy for Business Continuity and Disaster Recovery (BCDR). As an IT leader, keeping your employees connected and effective in the face of disruption or disaster is a critical priority.

Preventing major downtime due to catastrophic incidents such as floods, storms, earthquakes, system failures, and human error require special planning. To prevent business threatening downtime, companies of all sizes need to prepare for the worst, and that starts with understanding the importance of Disaster Recovery.

Why Wait?
Business Continuity,
the Backburner of IT Priorities

Sadly, Business Continuity and Disaster Recovery are often ignored by many organizations. Many businesses fail to prioritize 'what if' thinking, focusing instead on what they perceive as 'actual' realities. As such, investment and planning for disaster and disruption scenarios gets put on the back burner, and especially for small and medium businesses (SMBs), financial investment is curtailed because budgets are often tight.

Top IT Investment Priorities in 2019

According to CIO.com

1. Security
2. People/talent (training, acquiring, and leading)
3. Digital Transformation
4. Analytics/BI/AI/IoT/RPA
5. Cloud
6. Improve, lose, or replace activities relative to applications and infrastructure
7. Low Code/No Code
8. Business/IT continuity
9. Application upgrades
10. Getting more value out of previously made investments

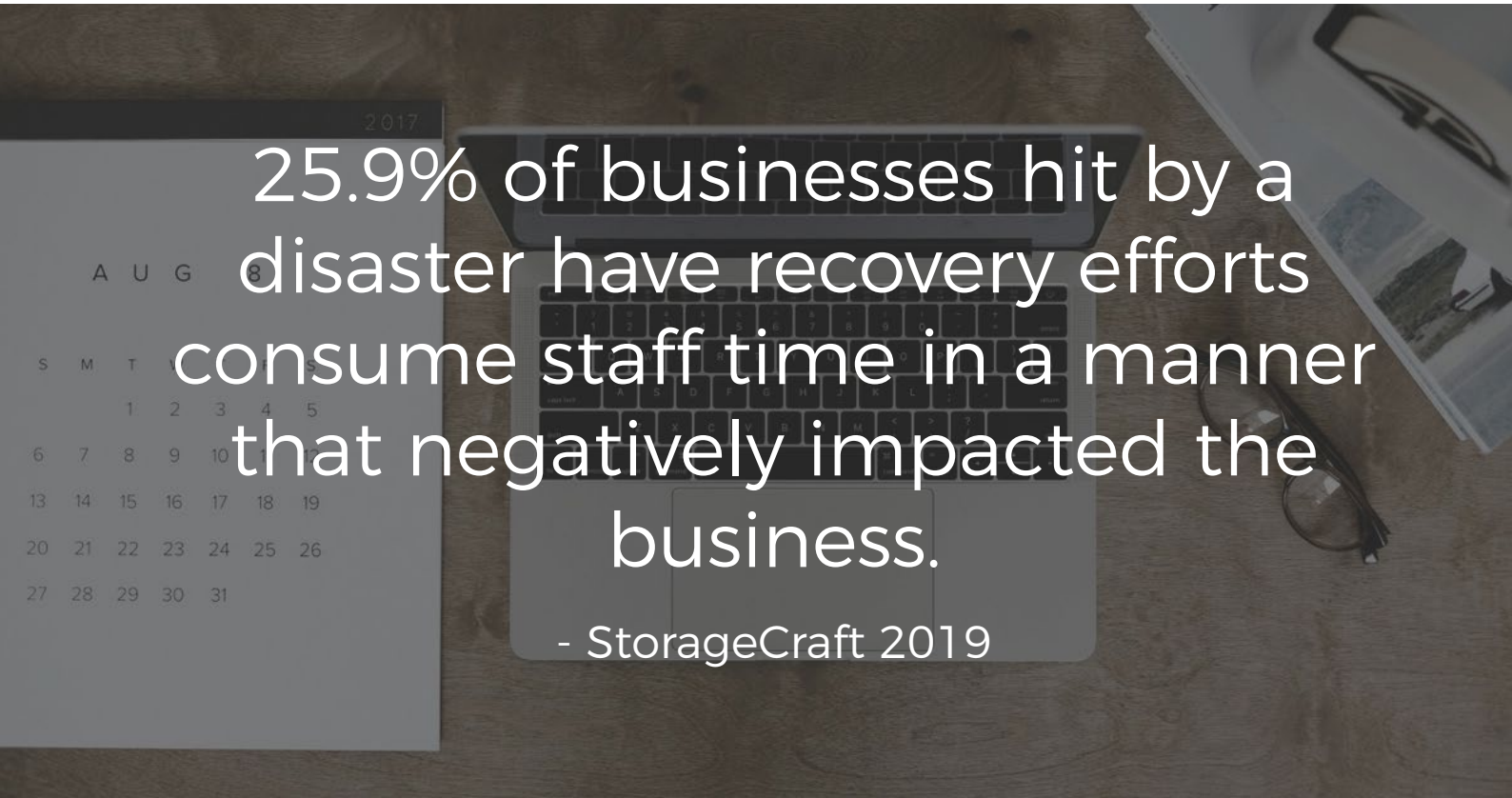
Busting Business Continuity & Disaster Recovery Myths

Business Continuity and Disaster Recovery (BCDR) can be tricky to define as they can mean different things to different businesses. However, a good place to start is by discussing what Disaster Recovery is not, since misunderstanding the true purpose of Disaster Recovery can be perilous for your business. Below are a few common myths relating to BCDR.

Myth #1: Having good backups doubles as a Disaster Recovery Plan

Backups are only part – albeit a critical one – of a good Disaster Recovery Plan. While backups are crucial for surviving a data loss scenario, they will be of little use if you cannot access critical applications such as email or billing systems in the face of a business disruption.

Data backups are simply the process of copying and replicating data from your core systems to another source or location. Today, many businesses have turned to cloud backups, as they deliver economies of scale for cost control, and cloud-based solutions often make it easier to restore data and can lower the risk of your backups being corrupted or damaged.



Myth #2: High Availability is the same thing as Disaster Recovery

Often, non-technical business leaders may think that if their systems are configured for High Availability, they do not need a Disaster Recovery Plan.

High Availability (HA)

HA refers to a system or component that is continuously operational for a long period of time. HA focuses on removing single points of failure and aims to build redundancy into your systems. This can involve multiple power supplies for your critical servers or redundant networking connections that allow you to stay online in the event that your primary connection is interrupted.

Disaster Recovery (DR)

DR is the process of recovering systems and access to business data when things fail. While HA and DR both work to solve the same problem (the business threat of downtime), the primary difference is that HA is designed to handle problems while your systems are up and running, while DR kicks in after your systems fail.

Myth #3 DR only deals with natural disasters such as fires, floods, or severe storms

Thinking about DR for your business often conjures up images of destructive natural disasters.

However, it's important to note that a good DR plan can actually help protect your business from more common events such as hardware/software failures at the system and user level, human error, and especially when it comes to securing your business against cyberattacks.

96% of businesses with a backup and disaster recovery plan fully recover from a catastrophic event.

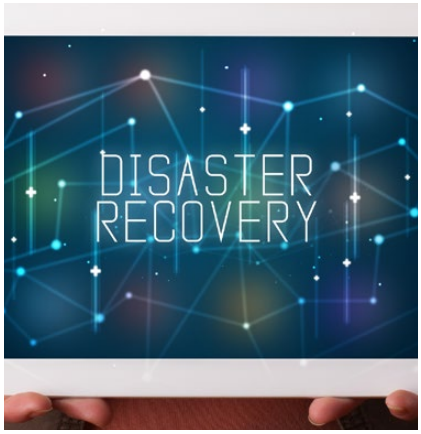
- Datto 2019

One thing that makes DR difficult to understand is the large amount of DR specific terminology that exists in the IT industry. In order to fully comprehend what DR planning involves and the role it can play in protecting an organization, business leaders should know the components of DR and Business Continuity.

A Disaster Recovery

Reference Guide

Below is a reference guide on the primary terms and components of DR, along with how they impact your business.

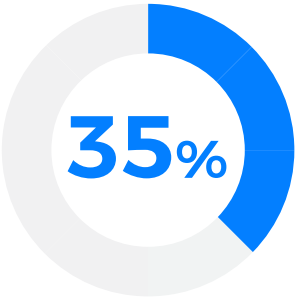


Disaster Recovery (DR) Plan

A DR plan is a set of procedures that describes how you will recover and restore your critical IT systems and data in the event of a disaster or disruption. This involves recovering important data and restoring your key systems (i.e. email, billing applications, etc.) so that normal business operations can continue smoothly and quickly after a major incident. DR is a subset of Business Continuity, where Business Continuity covers business resiliency as a whole, and DR focuses in on your technology systems.

Why does it matter?

Since technology is critical to the ongoing operation of any business, being able to quickly and efficiently resume operations with minimal data loss is essential. Most businesses cannot function without access to their core business applications and data, and DR planning aims to ensure that those systems can come back online as soon as possible after a major catastrophic event.



of organizations lost access to at least one mission-critical application after a catastrophic incident.

- StorageCraft 2019

Business Continuity (BC)

Business Continuity (BC) is the ability of an organization to remain operational with limited business impact in the face of a disaster or disruption event. Put another way, it's about resilience to stay afloat to prevent downtime, as opposed to planning a course of action to recover when something has actually failed. It's the planning to preserve operations; this often involves decisions such as where employees will work and how critical business changes will be communicated to employees in the event of a disaster.

Why does it matter?

Effective BC is incredibly important. Time is money! Most new and evolving businesses cannot afford or survive an extended period of downtime. Yet, smaller and new businesses commonly consider BC an afterthought, as the majority of their time and resources are dedicated towards productivity and real-time client demands.
Furthermore, many businesses have misconceptions about what BC is, such as assuming insurance or data backups alone can help. This causes them to be completely unprepared when a major incident occurs.

Business Impact Analysis (BIA)

A Business Impact Analysis (BIA) is the process of identifying the effects of a major interruption to your business as a result of any disruption or disaster. This requires taking a look at which processes and applications are central to the functioning of the business and identifying the potential impact if that system were to fail.

Why does it matter?

A BIA is critical if you want to keep your business resilient and engage in BC and DR planning in the right way. Without a proper analysis, it would be easy for a business to miss a potential issue, such as the impact to the business without a certain application. Skipping a BIA is a common mistake for small and growing companies. They often don't find it necessary at the time, yet when disaster strikes, they scramble to stay afloat.

Recovery Time Objective (RTO)

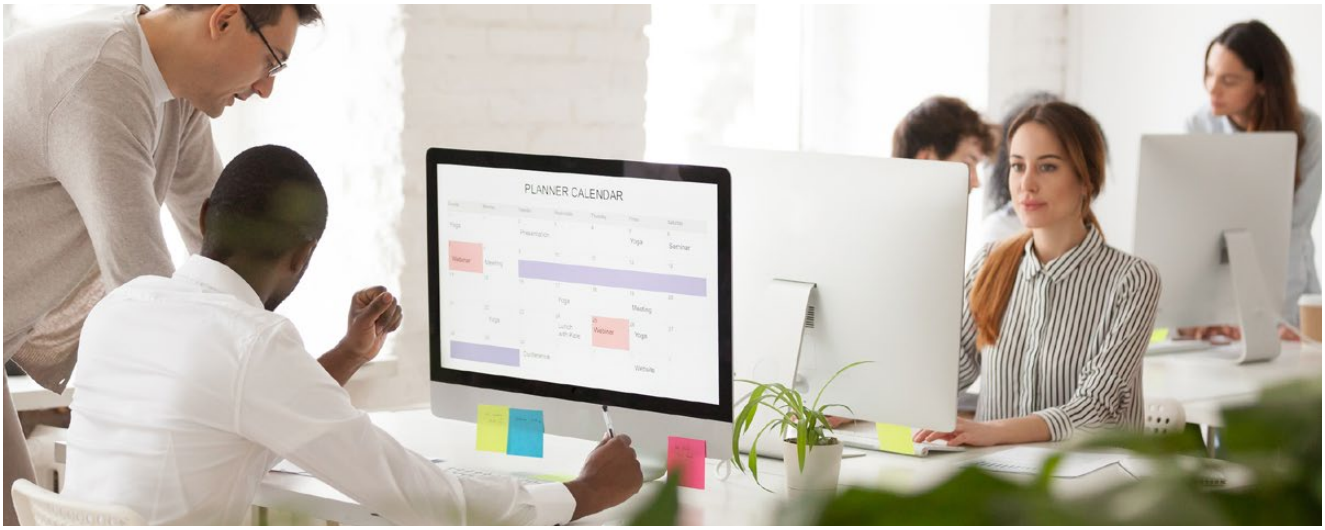
One of the true pillars of DR, a Recovery Time Objective (RTO), is the amount of time allowed between a critical outage and the restoration of normal operations for any given system or application. For example, an RTO of 2 hours for your ERP systems means that the system must be restored within two hours after a disaster, or your business may face long lasting repercussions.

Recovery Point Objective (RPO)

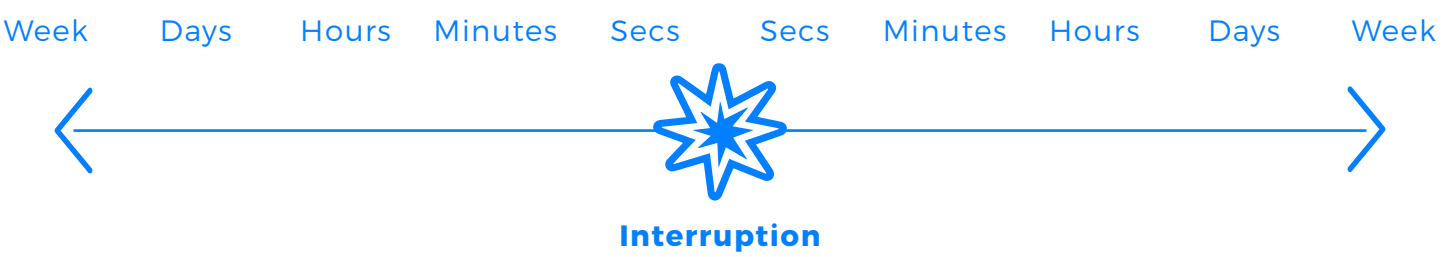
The second key metric of any DR plan, a Recovery Point Objective (RPO), is the maximum amount of data loss that is tolerable. Generally speaking, the more aggressive your RPO, the more often you are backing up your data and the higher the cost to maintain it. Put another way, your RPO reflects the amount of data you are willing to lose without significant harm to your business in case of a disaster or data loss scenario.

Why RTOs and RPOs matter?

RTOs and RPOs set measurable goals for your business when it comes to recovering from a disaster or major incident. They also force your leadership team to determine the importance of your critical applications and systems, which is significant when it comes to resuming normal business operations.



RPO vs RTO



Recovery Point

Recovery Point Objective

- Focuses on how you rebound from the loss of your data
- The interval of time between data backups and the loss of data
- Determines how often you should backup your data
- Considers how often your data changes

Recovery Time

Recovery Time Objective

- Focuses on your business as a whole
- How fast you need to recover your data
- Determines how much preparation and budget you need to recover
- Considers how much downtime you can handle

What are Critical Applications?

One of the main components of DR planning is identifying your core business applications and understanding how each application impacts business operations. This is critical when it comes to determining your RTOs, since restoring your most important applications first is the quickest way to get your business back on track after an incident.

Which application would impact you the most if it went down? Email is often top of the list for most companies. Are there any systems that you could survive without for a few days? When discussing the importance of your critical applications, ask yourself a few questions:

What do I need to contact key clients and business partners?

Which application is used by the majority of my business users?

Which departments would be the most impacted by the loss of critical applications?

Which applications are critical for processing orders for normal operations?

Data Backups vs Disaster Recovery

As previously discussed, data backups are a core component of a DR plan, but they should not be considered a DR solution on their own. Data Backups allow you to restore lost data and serve many purposes outside of DR, such as restoring files that have been accidentally deleted, satisfying compliance requirements, and recovery from a ransomware attack.

During a disaster, data backups play a critical role, as they allow you to recover data and resume productivity as quickly as possible. Cloud backups are a popular option when it comes to backing up your data as they can allow for quicker restore times, are scalable, and easier to manage as a third-party organization is usually dealing with day to day operations.

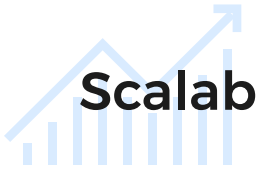
Having a managed backup solution is another viable option that can typically lower the impact of a major incident. **Below is a list of common benefits your company can receive from a Managed Backup Solution:**

Peace of Mind

Daily manual and automated backup testing ensures that backups are working properly and can quickly be restored when needed.

Guided Restorations

Restoring data, whether at bulk or granular restores, can be time consuming. Yet, with a Managed Backup solution, restores can be completed quickly, efficiently, and with zero impact to your core business operations.



Scalability

A Managed Cloud backup solution is generally scalable, allowing you to grow easily. With onsite backup solutions, storage may be limited, which can impact your ability to scale up.

Cost Effective

Managed and Cloud backup solutions require fewer physical resources on your end, which can lead to significant savings.

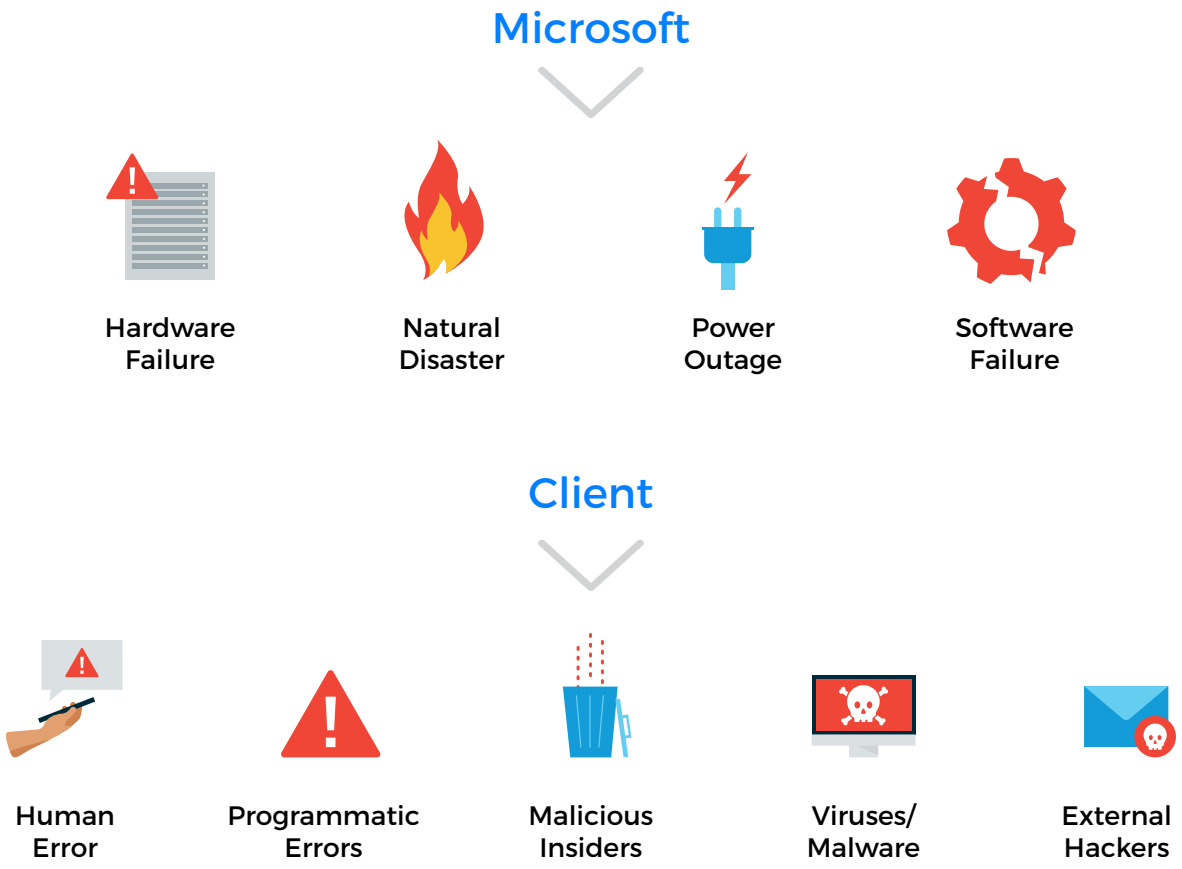
Improved Security

Generally, third party Managed Services Providers have a higher standard of security and compliance, which means that your data backups will be more secure.

Are You Backing Up Your Software-as-a-Service (SaaS) Applications?

With many companies turning to Cloud Services for storage, email, and critical business applications, it's important to understand what the SaaS vendor is responsible for and what you are responsible for when it comes to data resiliency and security.

SaaS applications such as Office 365 provide amazing productivity benefits, however, data protection is your responsibility, not Microsoft's. Below is a graphic that shows security priorities when it comes to the Microsoft Cloud.



In the above graphic, it is important to note that Microsoft's security revolves around uptime and the security of their data centres, while the client is responsible for their own data. It is a common misconception that Microsoft is responsible for client data.

When using **public Cloud services,** always make sure you understand **exactly what is being provided,** and ask yourself a few questions:

1. **How can I get support if I experience an issue and what level of support can I expect?**
2. **How quickly can I recover corrupt or lost data?**
3. **Am I taking advantage of all possible security features?**
4. **What possible risks am I facing and what can I do to negate those risks?**
5. **Do I have a plan in place to restore accidentally deleted items?**

Disaster Readiness Checklist

How Ready Are You?

Many companies find that when it comes time to put their DR Plan in action, they are not as prepared as they thought. Below is a quick checklist that can help any business assess their current Disaster Readiness process:

- ☐ **Develop RTOs and RPOs**
- ☐ **Define mission-critical systems**
- ☐ **Define required resources**
- ☐ **Establish a recovery event task list (i.e. a Runbook)**
- ☐ **Document current backup plans**
- ☐ **Create a schedule for updating your plan**
- ☐ **Measure, evaluate, and test**
- ☐ **Update your plan**

Where Will Your Data Go?

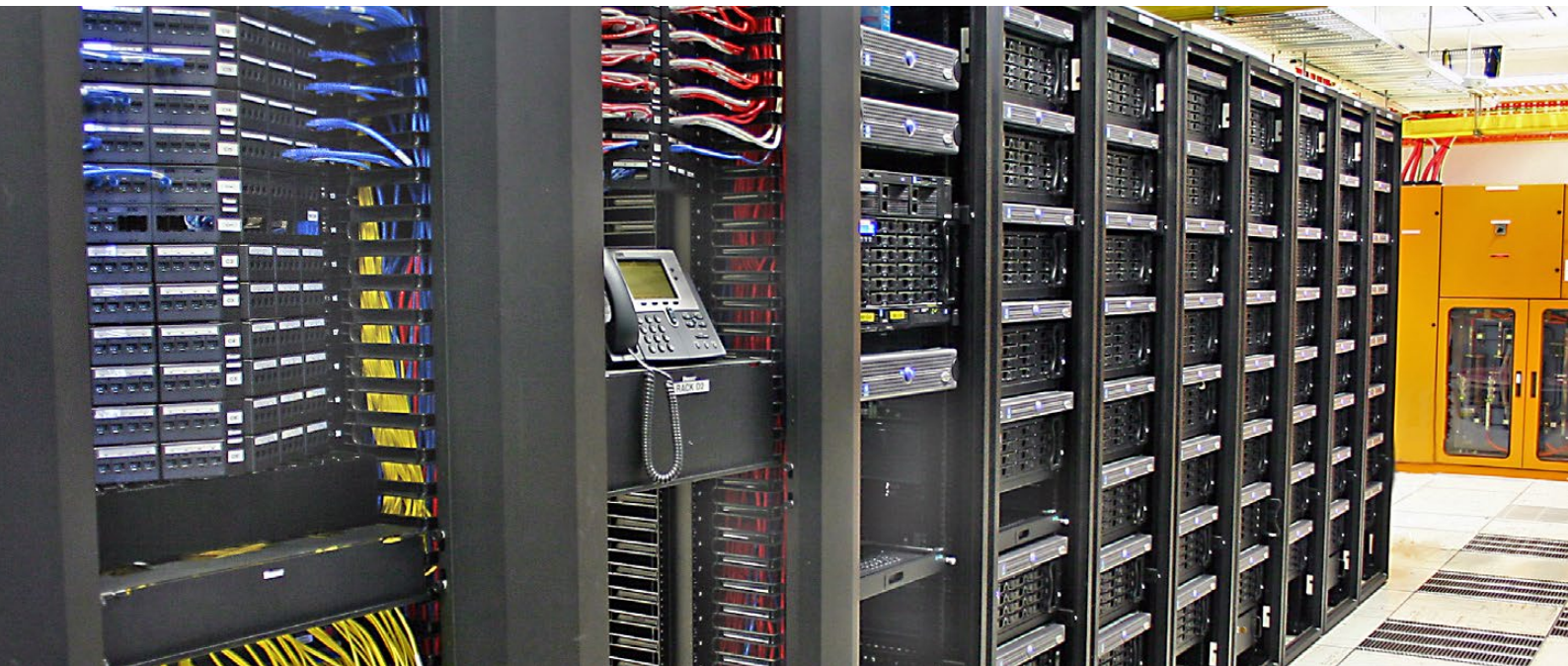
Understanding Secondary DR Locations

Another option that many businesses turn to when ramping up their DR practices is a DR site that provides a second secure location for their data and applications in the event that their primary data centre becomes unavailable. Most secondary DR sites are located at a significant distance from the primary data centre, which is done to ensure georedundancy.

When building a secondary DR site into your DR Plan, there are several important factors that need to be taken into account, such as:

- Data Backups
- RTOs and RPOs
- Network Connections
- Applications

A DR site is a popular option for businesses that cannot afford any extended length of downtime and ensures that productivity can resume at full capacity within a few hours after a major catastrophic event has occurred.



Alternate Workspace

Having an alternate workspace for employees to work from is a common form of BC planning. Alternate workspaces are not only designed to ensure business resiliency in the event of a major natural disaster, but can also help keep your business moving forward if your primary office space becomes unhabitable as a result of major construction or an accident such as a burst pipe, fire, or gas leak.

Alternate workspaces, at their core, provide basic office amenities such as workstations, chairs, and an internet connection, but more sophisticated setups can include separate and secure building access, meeting room space, and a dedicated washroom and kitchen facilities.

When selecting an alternate workspace, make sure to consider the following:

Location

Your alternate workspace should be in a safe location that is away from your primary facility and in a different power grid, but not too far away that it would be difficult for your employees to get to.

Size

Depending on your needs, you may want to consider an alternate workspace with a larger footprint, such as one that has separate meeting spaces and private executive offices. This can be important if employees need to call the alternate workspace home for an extended period of time. Proper space can allow for normal operations to continue without making employees feel cramped and uncomfortable.

Power

While your alternate workspace should definitely be in a separate power grid, your alternate workspace should also have several layers of resiliency built in, such as backup generator power.

Network Connection

A place to work doesn't mean anything if your employees cannot connect to their primary business applications. Ensure that you properly consider all networking needs well ahead of any time that you actually need to put your alternate workspace to good use.

Time to Test:
DR Testing

A complete DR test is an essential, yet often overlooked step of any BC plan.

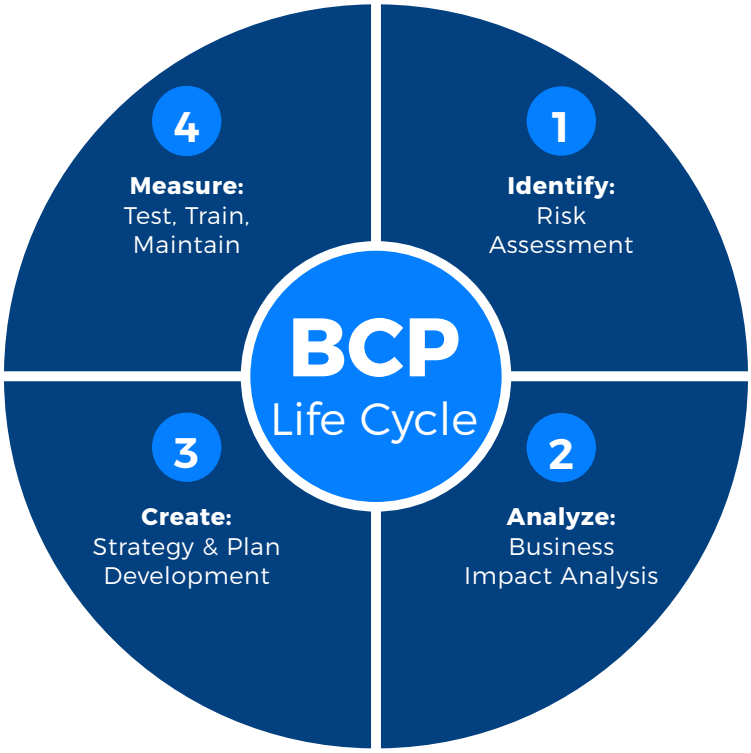
Often required as part of a compliance process or audit, a successful DR Test ensures that your DR plan can be easily enacted at a moments notice.

A DR Test will actually complete the failover from your primary data centre to the secondary DR site and test the time it takes to complete the failover. It will further ensure that every step along the way is working correctly.

One of the final outputs of a successful DR Test is the completion of the DR Runbook, a documented set of steps and procedures that covers every important piece of information required to successfully put your DR Plan into action.

The Road to **Resilience**

While a fully fleshed out DR plan can take time to complete, businesses need to make sure that they are considering BC early on and have the basic components in place for their employees to remain connected and productive.



Given the complicated nature of BCDR, businesses should consider outside help. Managed Services Providers can help with a variety of BC needs, including:

- Managed Backups
- DR Testing and Planning
- Alternate Workspaces
- Cloud Storage
- Security and Risk Assessments
- And more

Conclusion

Don't let a catastrophic event make your business another DR statistic. Let our team of experts ensure that your systems can be recovered and remain operational, no matter what happens.

IT Weapons has been helping develop DR plans and ensuring uptime for Canadian businesses for over 20 years, and utilizes Tier 3 data centres located across Canada to keep your business up and your lights on.

About IT Weapons

IT Weapons, a division of Konica Minolta, is a Canadian leader in secure cloud solutions and managed IT services.

Contact us for more information on creating a Disaster Recovery plan that works for you.

info@itweapons.com
www.itweapons.com