COPYRIGHT CIBECS 2022
This document is protected by international copyright laws.
Reproduction and distribution of this document without written consent from Cibecs is prohibited.

The IT Professional's Guide to Business Continuity and Disaster Recovery (BCDR)

Written by Cibecs - https://cibecs.com/endpoint-backup-security-quiz/

Objective: *The goal of this document is to provide the IT department with the tools required to build out a comprehensive BCDR plan that can be used to navigate potential disasters and mitigate potential risks and unnecessary losses.*

Executive Summary

There are two components that make up a business continuity and disaster recovery plan. A disaster recovery plan (DRP) and a business continuity plan(BCP) and both plans are essential to create a comprehensive framework that can be used to minimize disruptions of business operations in the case of unforeseen events.

- **Business Continuity Plan (BCP)**: Takes the entire organization into consideration when preparing for potential disasters. A business continuity plan is concerned with establishing systems and frameworks to deal with threat prevention and their impact on business operations with the goal to reduce disruptions.

- **Disaster Recovery Plan (DRP)**: Is specifically concerned with planning that relates to a business's IT department or function. The DRP has its own set of procedures and approaches that need to be implemented in the case of a disaster to protect the business's IT infrastructure and allow the business to return to operations as quickly as possible after an unforeseen event.

These projects focus heavily on prevention and risk aversion – outlining the investment the organization will make into precautions to ensure that the effects of a disaster are minimized and that they can easily resume business-critical functions

Business continuity and disaster recovery (BCDR) has become a vital aspect of enterprise IT as data becomes increasingly important and systems, networks and devices become more complex. There

are more severe consequences to business downtime and a growing number of possible complications and threats.

The consensus within the BCDR industry is that most enterprises are still ill-prepared for a disaster.

“Despite the number of very public disasters since 9/11, still only about 50 percent of companies report having a disaster recovery plan. Of those that do, nearly half have never tested their plan, which is tantamount to not having one at all.” - TechTarget

A holistic BCDR plan takes a broader approach than IT and takes the following factors into consideration, such as:

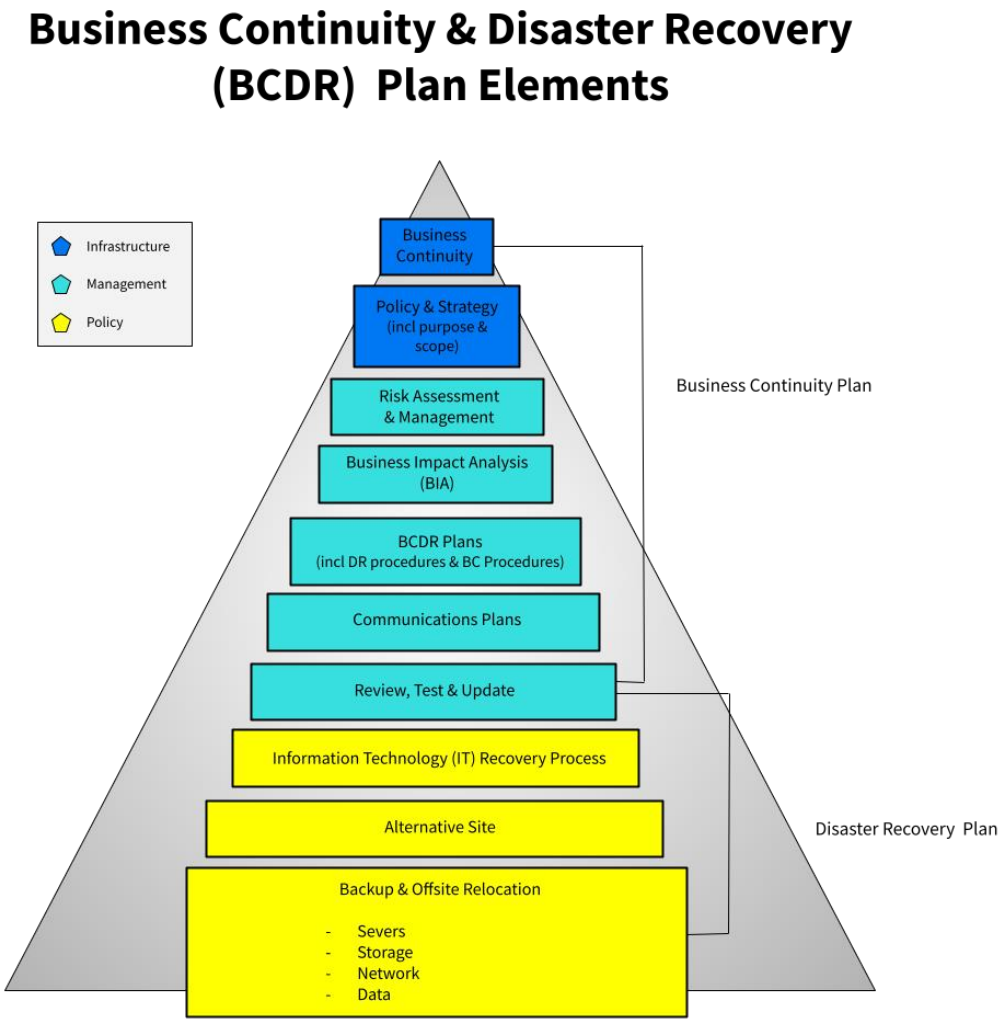
- Crisis management,
- Employee safety
- Alternative work locations

Common BCDR Threats

- **Geological:** Natural disasters caused due to dangers presented in a specific region such as earthquakes, volcanoes and tsunamis.
- **Meteorological**: Weather related natural disasters such as floods, wildfires, snowstorms, drought and so on.
- **Biological**: Pandemics, virus or illness outbreaks, food-bourne illness.
- **Accidental Man-Made:** Structural collapse of buildings or other infrastructure collapse, equipment failure, explosions or fire, water structure failure and so on.
- **Intentional Man-Made:** Bomb threat, terrorism, acts of war, theft/fraud, ransomware, technical sabotage, hackers and other malware that cause intentional damage or loss.
- **Technological:** Hardware or software failure, network failure or interruptions, utility failure.

Elements of a BCDR Framework

In this section we are going to break down the elements of a BCP and DRP and how they work together to create a comprehensive framework that ensures the future and profitability of an organization.



A BCDR approach requires thorough planning and preparation in order to create a strategy for achieving resiliency.

BCDR Plan Outline

The below table lists in detail all the elements that need to be included in a BCDR plan, and highlights which areas are included in the previously separate BCP and DRP. There are aspects of both a BCP and DRP that overlap and have to be considered when preparing your holistic BCDR plan.

BCDR Plan Elements		
BCDR Main Elements	**BCP Elements**	**DRP Elements**
Scope, Policy & Objectives		
Risk Assessments		
Business Impact Analysis - Prioritize business critical areas. - Establish an inventory of essential business activities for continuity purposes. - Create recovery time frame objectives (RTOs) to prioritize the implementation of recovery plans.		
Business Continuity Strategy		
Emergency Operations - Locations & Contacts		
Organizational Chart		
BCDR Team Establishment, Descriptions & Requirements		
Roles & Responsibilities		
Revision & Updating Schedules		
Emergency Response Plan		
Communications Plan		
Critical Business Information		
Plan Administration & Maintenance		
Plan Testing & Reports		
Implementing the Plan		
Instructions for Using the Plan		

Emergency Management Procedures		
Alternative Locations		
Backups & Server Offsite Storage		
External Communications		
Equipment/ Assets Inventory		
Insurance, Legal and Financial Concerns		
Testing, Validating & Updating		

BCDR Process

- **Risk Identification -** Understanding the types of risk an organization is likely to face no matter how unlikely.
- **Review of the organization's infrastructure -** the purpose of this is to understand what tangible and intangible assets the business has, and how to protect them.
- **Business Impact Analysis (BIA) -** Access potential scenarios and their impact on the business. Review with key stakeholders to ensure they understand the implications of these scenarios.
    - BIA areas used to analyze Business functions, processes and IT systems:
        - Business critical process assessment
        - Financial impact analysis
        - Operational impact analysis
        - Recovery objectives
        - Dependencies
        - Workaround procedures
- **Recovery Strategies** - develop documents, resources and outlines based on the BIA and determine a logical strategy based on established outcomes.
- **Plan Development -** develop and outline for your business's continuity plan, establish recovery teams and locations. Create a thorough BD plan and IT disaster recovery plan based on the assessment of damages.
- **Plan Implementation -** details how and who should implement the plan.
- **Review, Test & Update -** The best way to prepare is to map out possible scenarios, create test plans and implement them to check that they are effective to be sure the BCDR plan is effective in mitigating or reducing the impact of a disaster on the business.

Business Components

There are many parts to a business and what makes it a success, this is why it is vital that you ensure that you cover every aspect of the business when creating a BCDR plan. If you miss any aspect it could have a devastating effect on the longevity of the organization.

Business components that have to be taken into consideration when creating a comprehensive BCDR plan are;

- **People:** Such as employees, suppliers and customers are essential to creating a functional and profitable business, which is why these stakeholders need to be considered when establishing your BCDR plan. It is important for a representative from each business department to be involved in the creation of the BCDR plan as they have the knowledge about what is and isn't essential for the operation of their departments. Below is a list of business departments that should all have a representative involved in the process:
    - Data centers
    - IT infrastructure
    - Data security
    - Product development
    - Manufacturing
    - Inventory & storage personnel
    - Customer and vendor managers
    - Management & corporate governance professionals
    - Financial managers
    - Communications/ business representatives
- **Processes:** Are the lifeblood of a business they inform stakeholders on what needs to be done, how it should be done and why to get the best result and keep the business operating optimally. This means that mapping out the essential procedures required for the business to meet its obligations is necessary to know what to prioritize in the case of a disaster.
- **Infrastructure:** This includes all non-technological structures, such as equipment, buildings and any other assets that are essential in the business meeting its obligations.
- **Technology:** All technological infrastructure, programs and hardware required for business operations as well as all important data and information the business is responsible for.

Steps to Create a BCDR Plan

1. Create a BCDR team, establish roles & ownership
2. Perform a Risk & Business Impact Analysis (BIA)
3. Create a Prevention Plan
4. Outline Required Time Objectives (RTO) & Key Activities
5. Data Protection
6. Disaster Recovery Compliance Considerations

Step 1: Create a BCDR Team: Establish roles & ownership

Before beginning your DR Planning, ensure that you have established which individual is going to manage the project.

Project Leadership
Before you do anything else - decide who is responsible for establishing and testing your DR plan. This person will take ownership of the project and ultimately lead the research, testing and implementation projects.

Responsibilities & Requirements
This individual will draft the DR plan, make updates and changes as required and be able to lead the DR Team in case of requirement. They will need to communicate the plan to the company and ensure that all required resources are available and that staff understand their roles and responsibilities in the event of a disaster.

Step 2: Perform a Risk & Business Impact Analysis (BIA)

Before you can begin drafting your disaster recovery plan you need to conduct a thorough risk analysis of your environment. List all the possible risks that threaten system uptime and evaluate how imminent they are in your particular environment.

Anything that can cause a system outage is a threat, from relatively common man made threats like virus attacks and accidental data deletions to more rare natural threats like floods and fires.
DevX recommends that you "determine which of your threats are the most likely to occur and prioritize them using a simple system: rank each threat in two important categories (probability and impact.) In each category, rate the risks as low, medium, or high."

Create a Risk/ Probability/ Impact Profile
"For example, a small company (less than 50 employees) located in California could rate an earthquake threat as medium probability and high impact, while the threat of utility failure due to a

power outage could rate high probability and high impact. So in this company's risk analysis, a power outage would be a higher risk than an earthquake and would therefore be a higher priority in the disaster recovery plan."

By creating a thorough risk / impact / probability profile you prioritize different risks - and can more easily begin to branch from these scenarios into requirements.

This profile should not become an exhaustive list of every possible threat, but should instead provide a comprehensive and practical starting point for your DR strategy and Business Impact Analysis.

Your BIA is an outline of these risks and the probable impact on your company and systems. This then allows for effective precautions to be explored and threats to be addressed.

During this exercise you should also establish possible events and outcomes to help you better craft a thorough prevention and protection strategy. The purpose of this exercise is to help you find possible solutions to help mitigate the impact of a potential disaster scenario.

Below is a table outlining a few examples of how this can be done.

Business Continuity & Disaster Recovery: Scenario Map		
Scenario	**Description**	**Outcome**
A user's file has become corrupted.	A user's file has become corrupted or inaccessible and they need to restore it.	A user can restore a document in the event of corruption.
A user needs access to a previous version of a file.	A user has accidentally overwritten or deleted a file.	A user can restore a document in the event of corruption.
Ransomware Attack	The organization or user is infected by Ransomware and locked out of their data..	IT can restore a user from a previous snapshot before the ransomware attack. This includes their profile so that they are up in running in minimal time.
An employee's laptop has been lost or stolen.	Laptop has been stolen from boot of car/lost at the airport etc.	Unauthorized access to the data on the laptop is protected by encryption. IT can verify that encryption was enabled on the device. IT can track the last location of the device which may aid in the recovery of the device. The device can be remotely wiped by IT. Data Theft prevention will trigger and revoke access to data.
A user's computer has crashed.	A user's hard drive has crashed.	IT can do a full restore including profile settings.

		The user is up and running in minimal time.
Retain data for employees that have left the organization.	An employee has left the organization and the organization needs to retain access to the user's data for handover or legal hold.	The organization can retain the data and access the user's data if required.
Revoke access of suspended employee.	An employee is suspended and access to their data needs to be removed.	IT is able to remotely revoke access to the employee's data on the request from the organization.
Migration Scenario 1: ● **Hardware Refresh / OS upgrade -** A user's computer is migrated to new hardware. **Migration Scenario 2:** ● **Temporary device migration during repair -** A user needs to temporarily migrate to a device and access his data while his device is being repaired.	**Before Migration Process** 1. Time with user to locate data 2. Copy data to external HDD 3. Copy data to new device 4. Configuring Windows Profile & Settings 5. Setup & Configure Outlook 6. Install and configure custom apps **IT Time:** 4 – 6 hours **User downtime:** 4 – 6 hours	**After/ Outcome of Migration Process** 1. Install Discovery Agent 2. Live Migration 3. Update Migration 4. Install and configure custom apps **IT Time:** 30 minutes **User Downtime:** 30 minutes
Legal & Corporate Governance Compliance	A customer is required to prove compliance.	IT can demonstrate compliance for the customer **Prove that a policy has been implemented:** ● Can show the defined policy ● Show number of activated users **Prove a policy has been enforced:** ● Zero user intervention ● Show exact live number of protected users **Prove that you can proactively manage policy:** ● Report on unprotected users with errors to mitigate protection rating risks Retain data for an unlimited time frame (as required) for legal hold.

Step 3: Create a Prevention Plan

Once you have established your potential risks, the probability and the level of impact – you need to write a Prevention & Protection list based on your BIA.

This list serves as a basis for impact prevention.
For example:

The small company from California would list Power Outage as a potential Impact / threat and might employ an emergency power supply to mitigate the threat of Power Outage. One of the most crucial considerations for a DR Plan is obviously effective Data Protection The more preventative measures you establish upfront the better.
Money invested in solutions that ensure minimal impact – will be saved when it comes to recovery.
Employing effective Risk Prevention also improves customer trust and company image.

Meeting operational objectives should cause enterprises to closely examine the total cost of ownership of their PC's and find the point where keeping the old hardware will diminish returns.

* Remember that the immediate costs of preventative solutions are eclipsed by the savings made if a Disaster occurs.

Compiling a Prevention & Protection Strategy
Use your BIA and Impact List as a basis.

There are three common main focus areas:
- Data Protection
- Ensuring minimal system downtime
- Enabling fast & secure user data recovery

When compiling your list ensure that you correspond each potential High Risk threat with a solution and the cost for budget drafting and to present to decision makers. Ensure that each product or solution you present for prevention of DR Impact has been tested and approved by the required individual.

Calculating Threat Probability

Table 1 below illustrates an example of the model into which business IT can begin their threat analysis and prevention strategy.

TABLE 1. Threat Analysis & Prevention

Incident/ Threat	Probability	Impact	Prevention	Solution	Budget
Power Outage	High	High	Emergency power source	Solution x	$xyz
Data Loss **(endpoint first)**	High	High	Data backup	Endpoint solution y	$xyz
Data Loss **(server backup / off-site)**	High	High	Data backup	Server solution z	$xyz

The results should be a comprehensive list of possible threats, each with its corresponding solution and cost. It is imperative that IT presents all of these threats to the business operations units, so they can make an informed decision regarding the size of the disaster recovery budget (i.e., which risks the company can afford to tolerate and which it must pay to mitigate).

Cole Emerson, President of Cole Emerson & Associates, Inc., a business-continuity consulting firm, and chairman of the board of DRI International, believes IT "falls down" in its failure to communicate the real risks for system downtime to the business operations units of their companies. He says, "It's okay for operations to say no; it's not okay for IT not to let them know the risks."

Once you have prioritized your Incidents and Risks and listed the possible Threats you can begin to explore Prevention Solutions.

Step 4: Outline Required Time Objectives (RTO) & Key Activities

Extensive Planning

The key objective of a disaster recovery plan is to detail the key activities required to reinstate the critical IT services within the agreed recovery objectives. The most effective start point for any DR plan is the 'declaration of a disaster' once an incident has been deemed serious enough that 'forward fixing' at the primary location is impractical or is likely to result in an outage expanding beyond the maximum tolerable outage.

Defining Key Individuals & Service Providers

A description of the key roles and responsibilities must be compiled so that anyone assigned to a particular role in the recovery team understands what is required of them. Ideally individuals who are to be expected to perform a particular role should already be aware that they are likely to be called upon and should have received the relevant training. It is advisable to record the names and contact details of individuals in the relevant section of the overall plan.

Summarize Critical Services
Make a summary of the critical services, their recovery objectives and recovery priorities as well as third party contact details, particularly those that may be required to assist in the recovery effort.

5 of the Most Common Problems Associated with Disaster Recovery

- Data corruption, missing data or data loss
- Extended or unexpected down time
- Application performance issues
- Technical compatibility problems
- Data is not restored to the original location on OS

Detailing Recovery Activities & Processes
Include prerequisites, dependencies, and responsibilities. The detailed recovery activities should be held locally by the team responsible for performing these activities. The DR plan only needs to reference these documents, if you find it an absolute necessity to include these in your DR plan then do so as appendices and not in the main body of the document, don't allow the key purpose of the DR plan to be lost in unnecessary or duplicated detail.

Planning for Data Storage
By employing an endpoint data backup solution as the first step in your DR Preparation, you centralize your endpoint data and have an understanding of your data environment and your data requirements

Setting Time Objectives - Detailing MTO

- **Setting Your Recovery Time Objectives -** The recovery time objectives are based on how long the business can function without critical IT services – and this will involve prioritizing these IT services.
- **Maximum Tolerance Outage (MTO) -** A MTO must be established for different services and systems and it must be ensured in the plan that the goals and requirements around this are catered for. The recovery objectives must be based upon solid business requirements identified by the business impact analysis (BIA) process.

Prioritizing What is Business Critical
Mission critical applications and systems differ with different industries and companies operating within those industries. Decisions around prioritization should include business decision makers & allow for C-level input. This further ensures company-wide understanding of the importance of prevention & recovery solutions.

It is vital that companies seek legal consultation around Corporate Governance Compliance requirements and
their possible legal liability. This is specifically important when considering Data Loss & Secure Data recovery.

Testing Time & Velocity
Before compiling your MTO and time objectives, set up a number of tests to make certain that your requirements and objectives are in line with what is currently achievable. This also allows you to uncover possible areas in which you need to procure solutions to speed up processes.

3 Ways to Save Time During a Disaster Recovery Situation

- Ensure that everyone understands their role
- Have all the required contact details available
- Employ an advanced data recovery solution

Step 5: Data Protection

Protect Your Endpoints First
In Gartner's research (Q1 of 2009), it was stated that between 60 to 80% of an organization's data resides on desktops and laptops. In 2012, this figure was closer to between 80 to 90%.

In another Gartner report (March 2011, Gartner report ID#: G00211731), it highlights the importance of having an endpoint data backup and recovery solution.

It also explains the importance of selecting a "from the bottom up" technology (a new technology that focuses specifically in that space, ie. endpoint backup) rather than looking at traditional technologies which incorporate other backup methods (like a server backup which has a desktop component to it) which is modified to perform endpoint backup.

Use the "Best of Breeds" Approach
The "best of breeds" approach is recommended- specifically when considering a secure Disaster Recovery strategy. This means that your organization should be looking at the best solution for server backup, and the best solution for endpoints, not a consolidated solution.

Legal Requirements Regarding Data Protection
Most geographies have legislation that gives legal recognition to electronic documents and recognises that electronic documents and signatures can serve as the electronic functional equivalent of their paper based counterparts.

The impact of the widespread use of e-mail and electronic documents requires a paradigm shift in the way many of us think of documents. There are new risks associated with the use of electronic documents as they cannot be stored in a safe, like paper documents.

Organizations have a legal obligation to manage and retain documents and records
All companies are required to comply with the following two requirements:

1. All business related data must be protected from loss (e.g. hardware failure, human error or virus attacks), and
2. Data must be secure from unlawful access

Step 6: Disaster Recovery Compliance Considerations

Corporate Governance Compliance
Protecting data correctly and effectively is a paramount Compliance imperative. Not only do organizations with ineffective data protection strategies face the immediate costs and productivity interruption of data loss, they leave themselves vulnerable to data theft, unauthorized access to confidential files and are liable for legal penalties and criminal consequences due to failed corporate governance compliance.

Understand Industry Regulations in your Location
The recent penalty on BlueCross BlueShield of $1.5 million to the federal government is a harsh warning to the Healthcare and Insurance industries to ensure effective data protection.

Understand the legislation governing your industry, and ensure that you involve the Risk and Compliance Officer in your planning.

Not just I.T's Responsibility
The Board is responsible for risk management (including data risks.) It is necessary for them to demonstrate that they proactively manage these risks as a part of their duty of care.

At a minimum, the Board should disclose that there is a documented and tested process in place that will allow the company to continue its critical business processes in the event of a disaster.
It is the executives' responsibility to take effective data management seriously and protect the company's data, as the board is liable for negligence in this regard.

Consequences of Non-Compliance
- Severe reputational damage
- Legal disputes
- Financial penalties

- The appearance of ineffective internal management
- The loss of customer and staff trust

Data Protection Solutions

What should you be looking for in a Data Protection solution for a secure, effective and compliant DR Plan?

Best Practice Approach: The first step in your Disaster Recovery protection strategy should be employing an endpoint data protection solution that automates user backups and allows you control over the data being backed up to your server.

This centralizes all user business critical data and gives you the ability to perform educated capacity planning and understand your endpoint environment and real DR requirements.
With your endpoint data centrally backed up & secure - you can begin to plan for off-site replication and other DR Requirements.

What you Need: 3 Key Considerations:

1. A solution built to protect endpoint devices - use the best practice â€˜best of breedsâ€™ approach.
2. A solution that allows for central control over data backup policies & automates data backups.
3. A solution that simplifies the data recovery process - and makes it quick and simple to recover data in the event of a disaster.

Questions to Ask a Potential Service Provider

- Does your solution provide me with the ability to centralize all user data to our server - then allowing for server backup?
- Will your product provide intuitive central reporting, allowing IT to easily address potential risks?
- How quickly can we recover user data using your solution?
- How will your solution assist us with reducing support costs during the recovery operation?

While it is agreed by industry professionals that an endpoint data backup & recovery solution is absolutely imperative when considering your DR strategy, procuring the correct solution for your requirements requires finding a product Built for Endpoint Protection - to ensure that your business laptops & desktops are effectively protected.

BCDR Checklist:

BCDR (Preplanning)

- Establish the need for a BCDR plan.
- Map out your business continuity plan's structure (BCP).
- Define scope of legal and regulatory authorities & their requirements.
- Get key stakeholder buy-in
- Define a continuity & recovery policy statements, standards & define objectives.

BCDR Risk Evaluation & Control (Planning)

- Establish resource allocation.
- Identify & map out potential threats and risks the business faces due to certain events.
- Gather information on scenarios, solutions & potential outcomes.
- Establish safeguards & controls based on mapped out scenarios.
- Perform a probability analysis.
- Establish the requirements for protecting infrastructure, data & the organization's reputation.

Business Impact Analysis (Planning)

- Conduct a business impact analysis (BIA).
- Identify critical business functions and essential equipment required to continue with operations.
- Determine critical, time sensitive, business processes that will need to be prioritized
- Map out business function Interdependencies
- Establish RTOs (disaster and minimum acceptable level) and RPOs (last good data)
- Plan and coordinate data gathering and analysis
- Financial impact, customer impact, legal impact, regulatory impact
- Data backup strategies
- Prepare and present BIA Report
- Perform an IT Risk Assessment.

Develop BCDR Strategies

- Create a business continuity plan
- Create a IT disaster recovery plan
- Define what support services or resources are required
- Create a cost sheet for different outcomes
- Develop a cost/benefit analysis
- Regularly backup company data and secure data in the case of an attack or unforeseen disaster.
- Define recovery procedures.
- Perform regular backups & IT maintenance functions.

Emergency Preparedness & Response

- Establish emergency response plans.
- Identify & review existing response strategies, plans & procedures.
- Create a crisis management plan.
- Crisis communications plan.
    - Define methods of communication.
    - Define communication notifications and protocols.
    - Internal & external communications.
    - Key stakeholders to be informed (incl contact list)
    - Media spokesperson & detail their role
- Educate and inform stakeholders.
- Create an emergency contact list.
- Establish a disaster recovery team.
- Allocate roles and responsibilities to the selected disaster recovery team members.

Develop & Implement a BCDR plan

- Establish all the types of plans required, (DRP, BCP, IT Response Plan, Communications Plans, etc.)
- Establish alternative forms or channels of communication that can be used in the case of a disaster.
- BCP structure (base plan)
- Checklists
- Disaster recovery management
- Critical continuity functions
- Human resource responsibilities
- Recovery communications
- Insurance/Emergency funds
- Plan implementation
- Plan distribution

Stakeholder Awareness & Education (Post-planning phase)

- Awareness activities.
- Workshops & educational sessions.
- Training.

Business Continuity Plan Exercise, Audit, and Maintenance (Post-planning phase)

- Implement testing, validating and improvements based on outcomes.
- Exercise and test the plan.
- Walkthrough, backup, integrated, comprehensive, standalone, call trees, line of business, facilities.
- Timeline for RTO & Key activities.
- Maintain BCDR plan.
- Establish an audit process.

Conclusion

Undertaking a BCDR project and formulating the best and most effective preventative strategies for your enterprise takes considerable planning and research. However the challenges of optimizing these operations, ensuring that costs are controlled and minimizing user downtime can be answered with the right solution.

Find out more about Cibecs can assist you with managing, protecting and securing your endpoint data and meet your regions compliance requirements by visiting https://cibecs.com/endpoint-backup-security-offer/ and lock in our special offer.

Special offer has limited availability*