IT DISASTER RECOVERY PLANNING EXPLAINED

In today's digital world, technology disruption for even a few hours can result in significant financial consequences to your business. According to Gartner, the average cost of IT downtime is $5,600 per minute. (That's more than $300,000 per hour!) For large organizations, that number tops half a million dollars.

It's no wonder that having a well-designed and effectively maintained disaster recovery plan in place will substantially increase your ability to recover lost data and return to normal operations as quickly as possible.

So, let's look at strategies for developing a disaster recovery plan that will protect your organization.

(This article is part of our Security & Compliance Guide. Use the right-hand menu to navigate.)

Business Continuity Planning vs Disaster Recovery Planning:

Business continuity planning (BCP) and disaster recovery planning (DRP) are sometimes used interchangeably. And while they are interconnected, the two are different concepts:

- Business continuity planning is the overarching strategy that covers the entire company to ensure that mission-critical functions can continue during and after unforeseen events. Such events could include natural disasters, death or illness of a company executive, a security breach, and more.
- Disaster recovery planning is actually a subset of overall business continuity that helps ensure organizational stability following an impact to IT only. Examples include disruption to servers, desktops, databases, applications and so on.

(*Compare business continuity to business resiliency.*)

Goals of disaster recovery planning

When crafting the right disaster recovery plan for your business, it's important to first assess the goals you'd like the plan to accomplish. The purpose of the DR plan is to protect users and the business from financial, legal, privacy and security related repercussions of a disaster incident.

Let's look at the key reasons to plan for disaster recovery.

Mitigating risk

To contain the extent and scope of the disaster impact. Conduct a thorough risk assessment and evaluate various targets. Design the DR plan to isolate mission-critical systems and streamline the risk mitigation and remediation pipeline.

Reducing disruptions

Service availability is critical to business success. A primary goal of a DR plan is to ensure that systems return to normal and optimal performance soon after downtime. Metrics such as Mean Time to Recovery (MTTR) should be optimized within disaster recovery planning.

Reducing economic impact

Prioritize MTTR of IT assets based on the perceived business value. An optimal disaster recovery strategy is focused on:

- Systems that directly impact the cost of downtime
- Critical services such as infrastructure and healthcare applications
- The wide extent of the user base

Preparing for disasters

Getting ready for disasters waiting to happen. Cyberattacks are getting more sophisticated by the day—which means you can always improve your ability to handle the next wave of security threats.

Understanding cybersecurity posture

Cybersecurity is hard. It is time and resource intensive. You need to:

- Get started with the right cybersecurity strategy
- Secure the most important IT assets
- Identify new vulnerabilities
- Patch zero-day exploits as soon as they are found

It's also important to neither overestimate nor underestimate your cybersecurity strength. Understanding your cybersecurity posture helps optimally allocate resources to prepare for and respond to disaster incidents when needed.

Achieving regulatory compliance

Organizations should be well prepared in adapting to the changing regulatory environment. A disaster recovery plan should be a part of the compliance strategy as it alleviates risk and provides a systematic approach to recover from disaster situations. Critically, compliance is mandatory for organizations in certain industries, including:

- Healthcare
- Finance
- Defense
- Infrastructure

(Understand governance, risk & compliance, known as GRC.)

Maintaining brand loyalty, reputation & user trust

Internet users today are increasingly aware of their rights to data security, privacy, and control. A DR plan ensures that your users maintain access to their data even when disaster strikes.

As a result, service providers maintain trust and brand loyalty necessary to survive the competitive Internet market landscape.

Who creates the Disaster Recovery Plan?

Now let's look at creating the plan itself.

Before you begin mapping out your DRP, it's important to have the right people in place to lead the charge. To this end, establish a disaster recovery plan committee which includes key decision makers from across the entire organization:

- Top management
- IT management
- Human resources
- Finance
- Security
- Vendor management

Collectively, these individuals will be responsible for outlining, implementing, testing, and

maintaining the disaster recovery plan.

How to create a Disaster Recovery Plan

A disaster recovery plan can include an exhaustive set of actionable guidelines for all employees responding to a disaster situation that may impact corporate IT networks and systems. The Disaster Recovery Planning (DRP) document is your roadmap to implementation—as such, you should update it regularly and store it a safe, accessible storage location in event of emergency. (If it's in the cloud, but your internet is down, how can you access it?)

You can follow a Disaster Recovery Planning document template given below to ensure that your workforce can easily understand and adopt the systematic actionable guidelines to protect against disasters:

Step 1: Define goals

Identify your business goals. Associate a business value to your services, systems, departments and organizational functions, and how IT availability impacts various business operations.

Step 2: Define responsibilities

Who is in charge of what? Develop an organizational chart and define the responsibility of each individual involved in executing a DR plan.

Step 3: Prioritize application assets

Identify critical applications and assets. Focus your DR efforts in order of priority based on business value, user impact, legal requirements, ease of recovery, and other applicable factors.

Step 4: Describe asset details

Maintain an exhaustive directory providing details on every asset including vendor details, models and serial number, cost, number, and other relevant details.

Step 5: Define backup plan

Describe the frequency and schedule of backups. Different libraries and directory objects may be processed for backup at different schedules and volumes based on data storage and transfer cost, speed, business, and legal value.

Step 6: Define recovery procedure

Define actionable guidelines focused on three key elements:

- **Physical damages:** emergency response to fire incidents or natural disasters.
- **Data backup:** Execution guidelines of the data backup plan.
- **Recovery:** Restoration of data assets from backup storage locations.

Step 7: Plan for mobile & hot sites

Establish alternative (hot) and mobile facilities to handle the DR operations while the home site is reestablished. This is particularly useful when physical disasters are involved.

Step 8: Establish restoration guidelines & framework

As the data is recovered from backup sites, how to reestablish the original site, systems, and operations to an optimal state.

Step 9: Test, test, test

Thoroughly test and evaluate your DR plan. Perform DR drills and training sessions to prepare your workforce for potential emergency situations.

Step 10: Continual Improvement

Continuously assess, improve and update your DR plan. Keep your records and procedure up to date with respect to risks and resources available to the organization.

Time is critical for disaster recovery

If your organization hasn't created a disaster recovery plan or hasn't made it a priority to maintain or improve upon it, then time is of the essence. No business can afford to have an ineffective response to unforeseen circumstances, and once a disaster occurs it's too late. A disaster recovery plan can be the difference between the survival of your business or becoming another statistic.

To avoid costly delays in service, plan your disaster strategy by thinking about goals, performing necessary audits, planning for contingencies and partnering with a third-party vendor, if needed.

Related reading

- BMC IT Operations Blog
- BMC Security & Compliance Blog
- Disaster Recovery for the Cloud
- What Is Threat Remediation? Best Practices for Remediating Threats
- Worst Data Breaches Today: Critical Examples
- The Basics of Business Continuity Management (BCM)