Google Cloud

Plan for business continuity

You've recently learned how business continuity is an organization's ability to maintain its everyday productivity by establishing a disaster recovery plan. You've also learned about two important types of plans to help a business keep their operations going: a business continuity plan, or BCP, a document that outlines the procedures to sustain business operations during and after a significant disruption; and a disaster recovery plan, or DRP, that allows an organization's security team to outline the steps needed to minimize the impact of a security incident.

To create an effective BCP and DRP, you need to work together with your cloud service provider and have a clear understanding of your responsibilities and your provider's responsibilities.

In this reading, you'll drill down into business continuity and disaster recovery planning, and get examples of how to identify what needs to be protected and what can be done to recover it in case of an emergency.

The organization and the provider

Your CSP is responsible for ensuring the availability of your organization's data to the degree specified by the shared responsibility model, even in the event that one of its data centers experiences downtime. To manage this responsibility, your CSP keeps the hardware running in certain regions, typically by configuring their platforms to maintain data processing even in the presence of disruptions or outages in specific data centers, and making sure traffic can be diverted to a working data center if one of its data centers goes down. However, if an entire region experiences an outage, organizations relying on the cloud service may encounter application programming interface (API) processing interruptions and unavailability of databases or virtual machine (VM) instances.

Some cloud service providers have a failover data center set aside to take over when the data center stops running. While other CSPs, like Google Cloud, have multiple data centers running at the same time in each region.

Your organization is responsible for the data beyond the infrastructure. This includes tasks such as data governance, access control, data backup and recovery strategies, as well as compliance with data protection regulations.

Cloud service provider business continuity and data recovery plan example

An example of a cloud service provider that has a BCP and a DRP is Google Cloud Storage. Google Cloud Storage functions in a large, multi-region geographic area such as the USA, and takes measures ensuring that data will still be available, even if a particular region experiences an outage. For example, if a region on the west coast of the USA is not available, the data stored in Google Cloud Storage is still available from a different region.

CSPs like Google Cloud Storage don't share their full BCPs or DRPs with individual users, since these plans may include sensitive customer information. However, users of the service can rely on Google Cloud Storage to utilize their BCP and DRP plan to ensure that the service is resilient to a zonal or regional outage, depending on the deployment of the service in the customer's organization. The CSP is also responsible for testing its platform and providing updates to it as needed.

A BCP and DRP plan in action

When a cloud security team develops its BCP and DRP, the team needs to make sure to document every aspect of the plan, including a business impact analysis, BC and DR strategies, roles and responsibilities, and tools and resources. The documents should be kept in a safe place, but where they can be accessed quickly. Building a BCP and a DRP plan is a team effort, including. the teams in an organization, and teamwork between the organization and its GCP.

In addition to documentation, communication is also a key component of any BCP and DRP plan. A cloud security team needs to communicate the plans to all employees and other stakeholders. This will help ensure that everyone knows what to do in the event of a disaster.

In the following example, you'll follow along as the cloud security team for a company, Cymbal Bank, creates their BCP and DRP plans. Here are the steps the team takes:

1. Conduct an audit of their distributed platform.
2. Organize their apps into three tiers, based on the criticality of the apps for Cymbal Bank's core business:
    a. Tier one apps include user-facing apps that deal with sensitive data
    b. Tier two includes important internal or regional applications like Human Resources (HR) or finance
    c. Tier 3 includes departmental applications dealing with external data like public docs on their website.

3. Assign recovery time objectives and recovery point objectives to their apps and data, so they can focus their solutions on bringing the most important resources back online quickly.
4. Conduct a risk assessment on the whole system to identify workarounds to potential risks, and document them.
5. Documents all communication contacts, including everyone involved in the plan, and what everyone's duties are in the case of a disruption.

Once the audits, checks, risk assessment, and documentation are done, the team presents information about it to company leadership. In their presentation, they discuss how they can continue work if the cloud provider goes down. Finally, the organization tests out their BCP and DRP plans to let the team practice their approach in the event of an incident and identify gaps in the plan. This allows them to address the aspects of the plan that need to be improved.

During and after the simulations, the team keeps a record of everything as it happens and focuses on any weaknesses in the plan they can fix.

BCP and DRP templates

As a security professional, you should consider using templates to build effective BCP and DRP plans. The templates will include key placeholders for you to fill in some of the information before you perform simulations or tests. This information should include:

- Summary
- Objectives
- Roles
- Disaster response planning
- A communication plan
- Steps for testing the plan

Here's a bit more detail on what goes in the Summary, Objectives, and Roles sections of a BCP:

Summary

A summary of a BCP can help an organization's members grasp the essential information in the plan. The summary also gives members enough information to understand what their roles are in the plan.

The summary should include the purpose for the plan, discuss the steps taken in the plan, and briefly describe each team or individual's role in the plan. A summary should be one page or less, since you want to present the ideas quickly. You'll go into more detail in the plan itself.

Objectives

The objectives of a BCP clearly describe the intended results of the plan and provide a comprehensive outline of its steps.

Here are some objective examples in a BCP:

- Create a schedule for regular backups of vital data-so if there is a system failure, the data will be safe.
- Grant least privileged permissions to those who need the access.
- Determine who is responsible for which parts of the plan. Detail what the CSP is responsible for doing and what is the company responsible for doing.
- Create a list of workarounds, and determine how you can use them to keep the company operating normally.
- Ensure that critical applications are brought back online during a disruption event within four hours.
- Avoid loss of data for such applications that exceeds one hour.
- Ensure that customers can place orders again within a certain period of time.

Note: Objectives will be specific to the situation and the needs of the organization. They will differ depending on the context.

Roles

Every member of the organization has a role to play in the case of an emergency, like a major cloud service disruption from an attack or a natural disaster. Communication throughout the organization and within the team are vital. It's important to have a pre-established communication plan so teams can work together effectively during unforeseen circumstances.

Key takeaways

BC and DR planning are crucial for organizations to maintain productivity during and after significant disruptions. When a cloud security team builds a well-defined plan, often in collaboration with a cloud service provider, it clearly outlines responsibilities and measures to ensure service and data availability. Effective documentation, communication, and teamwork between the organization and the cloud service provider are vital components of BC and DR planning.