

# IPMountain

Local Presence, Global Impact

IPMountain Security Analysis

# IPMountain

*Local presence, Global impact*

## Environment Evaluation

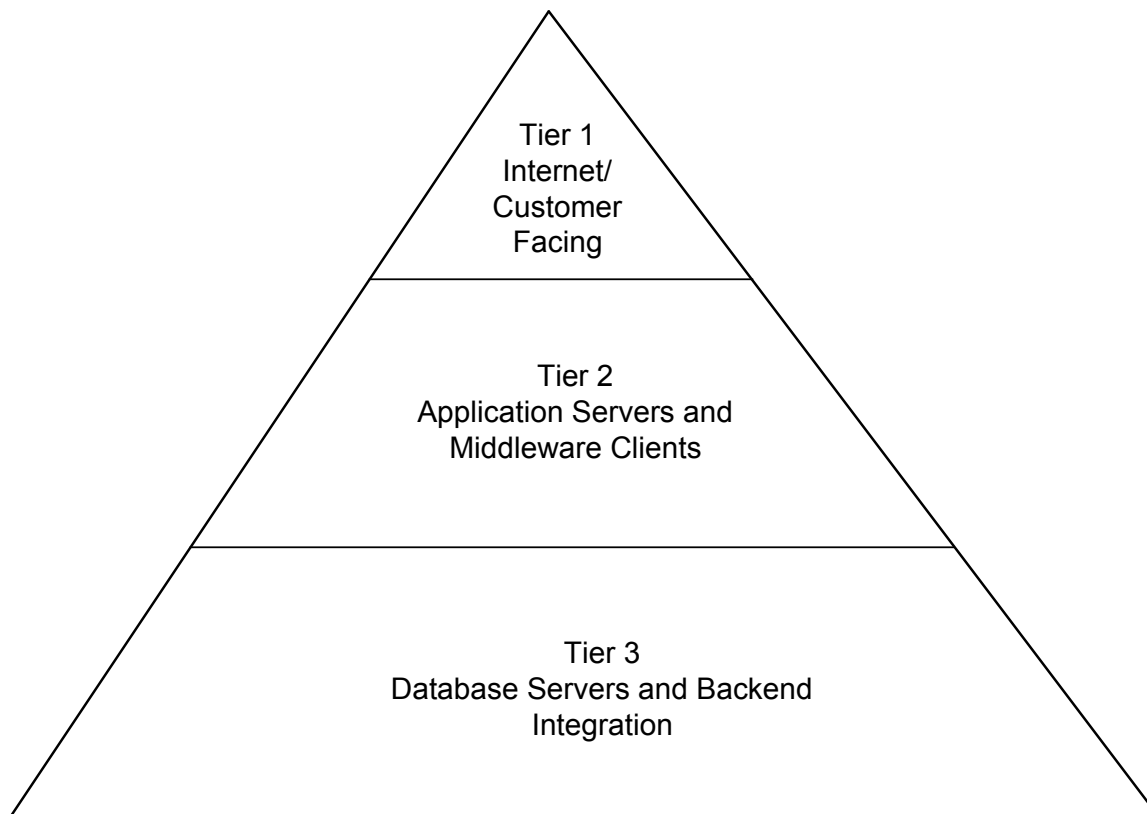
Disaster Recovery (DR) starts with a complete understanding of the user environment. Many aspects of data usage must be analyzed and understood so that an effective DR strategy can be designed and implemented. Some of the areas are:

1. System architectures.
  - a. Hardware types
  - b. Network topology and IOS levels
  - c. Operating system type and levels
  - d. Database levels and functionality.
  - e. What hardware resources are available at end user locations for DR?
2. Organization Policies and Service Level Agreements (SLA)
  - a. What data needs to be recovered.
  - b. Acceptable down times.
  - c. Acceptable loss of data.
3. Critical Functions
  - a. What is needed for business survival?
  - b. Who controls/is responsible for the functions?
  - c. Public perception of critical functions.
4. Organization Skill Level
  - a. How big of a role will the end user take in recovery?
  - b. What training is needed to bring the end user up to appropriate levels of skill?
  - c. What technical resources are available at the end user?

These and other areas must be fully documented and understood in order to complete an effective DR plan.

## Infrastructure Build Out

Building an infrastructure to Support DR would mean a significant investment. A multi-tiered information technology environment would have to be constructed and very strict security measures would have to be implemented. The following diagram attempts to visualize the type of environment needed for effective DR:



The multi-tiered environment allows for flexibility, scalability, and security implementation. The following is a description of the tiers and how they apply to DR:

Tier 1: This tier faces the public Internet or end user environments and is the least secure. In this tier we would place web servers or connectivity servers that would facilitate access to the wedge.

Tier 2: This is the tier that hosts the applications that perform data replication and data storage services. These applications can be customized to end user requirements or be third party applications designed for data replication and storage.

Tier 3: This is the most secure tier and hosts the database servers which provide standby databases and information tracking for DR. These databases can be customized to meet end user requirements.

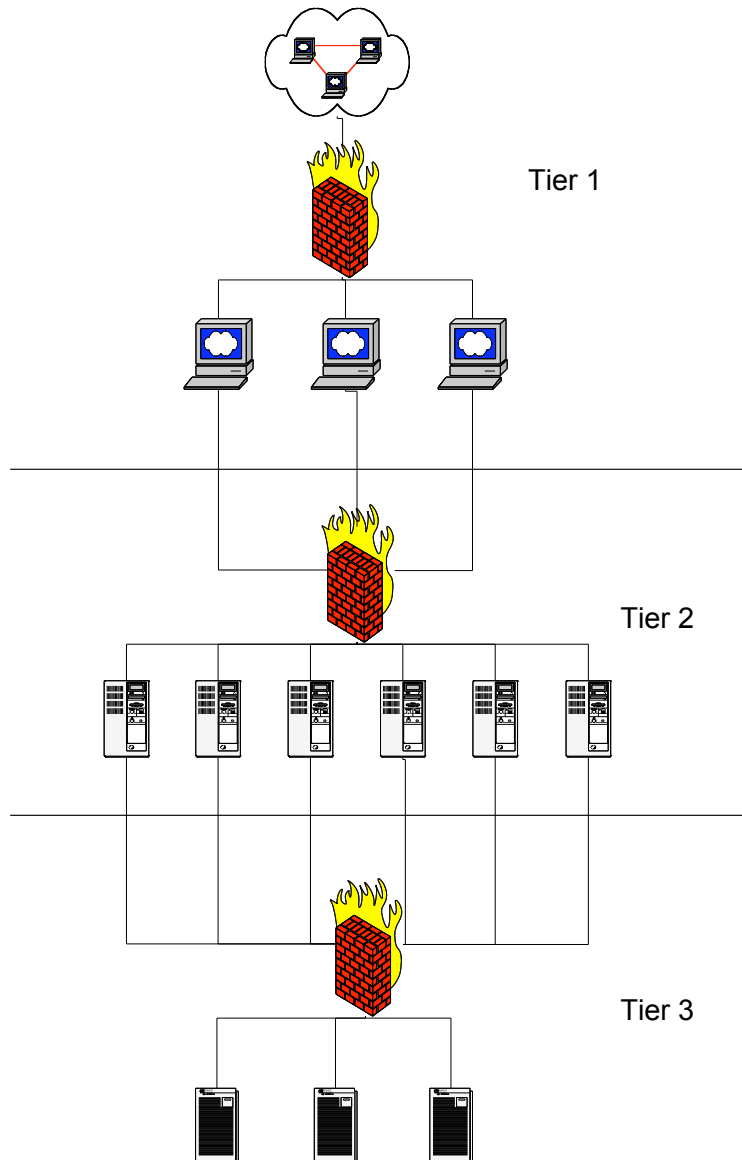
Each tier would be protected by routers running access control list (ACL) and firewalls that implement very strict security policies that are define appropriate for each tier. Administration access to the wedge is restricted to only internal technical staff and is audited on a weekly basis.

The server for each tier would be selected based on end user or vendor requirements.

## **Data Replication**

Data replication is the process that is used to provide current snapshot of data for end user disaster recovery. This process must be defined with end user requirements. The following attempts to describe the process:

1. A standby database will be configured in tier 3 that makes the end user schema.
2. Replication of the database is handled by application servers in tier 2 that use secure connections to database servers in tier 3.
3. The application servers use secure connections to end user environments through tier 1 devices.



## Data Backup and Storage

Data storage would be accomplished through the use of a Storage Area Network (SAN) and Network Attached Storage (NAS) and offline data storage devices.

The SAN could be an EMC Symmetrix or equivalent systems.

There is a variety of NAS solutions available. A full evaluation of requirements would determine the types of NAS to be used.

Off-line storage could be accomplished through the use of a SUN L-700 or a STK device. These are mass storage devices used to back up the SAN and NAS.

A procedure for defining SAN and NAS for customer use would be defined. The procedure would cover the following areas:

1. Amount of storage required.
2. How to connect to application servers in tier 2.
3. Frequency of data replication or data back up.
4. Off-line tape storage (where do we store the tapes used in the off line devices).
5. Length of on-line store (how long will data stay on the on-line devices before being moved to off-line storage).
6. How do perform and restore in the event of a disaster.