A data center for the core of every organization making use of IT as its basic business or as a supporting arm. All the business critical information lies in the data center components. With the growing interconnectivity among the businesses and internet and the prevalence of hacking and corporate espionage, securing the data has become the key to survival of an organization. A breach of the data center can have catastrophic consequences to the business. Hence securing the data center is a prime concern in the current scenario.

The overall architecture of the Data Center is essentially comprised of the following four layers:

1. **Network**: The network layer uses Layer 2 and 3 switches to provide reliable access to the compute layer. It connects all the data center resources. It uses Layer 2/Layer 3 network switches to connect users with data center resources.

2. **Compute**: The compute layer is composed of the servers that run applications invoked by users. Server switches interconnect the computing resources and provide access to the storage layer.

3. **Storage**: The storage layer stores the data used by applications on storage subsystems like disk and tape drives. The storage layer uses storage switches and optical transport platforms to interconnect and provide access to storage resources within the data center.

4. **Security**: The security layer is composed of the specialized security software that run across all the other layers of the data center in addition to being present in the form of specialized hardware like firewalls, Intrusion Protection System (IPS) etc.

In order to have well defined defense setup against information security risks, multiple layers of
security with different technologies have to be inbuilt into the design of the data center
The overall security deployment happens in stages as described below:

**Stage #1: Security Policy Definition**

For a comprehensive security envelope, security controls have to be inbuilt into each of the data center layers. These controls have to be defined in alignment with the required security compliance levels and best practices for data security. These controls are defined in the organization's Information Security Policy. This document states how an organization intends to protect its information assets.

When defining a policy, the following elements have to be considered:

- Objectives, or what you want to accomplish with your security policy.
- Scope, or who and what your security policy should cover. Your policy should state who can perform an action, not who cannot perform it.
- Data, or what needs to be secured.

**Security Policy Definition considerations**

Some of the aspects to be considered while defining the security policy are mentioned below:

1. The Security Policy definition exercise is initiated by the Information Security Manager of the organization with the heads of the various technical towers and other stakeholders (network, windows, UNIX, storage, backup, administration etc)
2. Identify the regulations and practices that influence your security needs. This information can come from the following types of sources:
   - Government or industry regulations or standards.
   - Requirements of the stakeholders in the security of your business.
   - Possible threats to your security.
3. Identify the various roles individuals play as they interact with the data protected by your security policy. To help identify these roles, determine the following:
   - The types of individuals who are interacting with the data assets.
   - The nature of the interactions between the individuals and the assets.
   - Who will be the audience of the policy
4. Business Requirements: One of the key factors while formulating a security policy is the business requirements of the organization. Security is based on the triad of “Confidentiality”, “Availability” and “Integrity”. From a business point of view, the security should not be a factor that effects the availability of the business.
5. The policy types:
   - Technical Policy: For the consumption of the technical administrators and are to be used on an overview level for the technical activities.
   - Governing Policy: Defines the high level aspects of the security and is focused towards the managers and end users
   - Job Aids / Guidelines: These procedural documents with the step-by-step directions of how the policy statements have to be carried out.
Based on the above points, the draft Information Security Policy will be defined. The policy has to be reviewed and finalized. The policy should provide guidelines each of the four layers that exist in the data center. Appropriate controls mechanisms should be defined to ensure that the guidelines are followed.

Regular review of the Security Policy should be planned to cater to the changing Information Security paradigm.

**Stage #2: Implementation of Security Policy**

As mentioned earlier the architecture of a data center consists of:

1. Network
2. Compute
3. Storage
4. Security

The information security in a data center environment is not limited to putting in the security components in the network. Dependable Information Security can be expected only when security is embedded into the design of each of the architecture components. The security principles to be kept in mind while designing these components are Data Center include:

1. Authentication
2. Authorization
3. Confidentiality
4. Integrity
5. Availability

All the security implementations have to be done in accordance with the Information Security Policy.

**Network Layer Security Considerations**

- Network components include routers. Switches, firewalls VPN Concentrator etc. They are the backbone for all the data flow happening in the organization.
- The design of the network must cater to the points defined in the organization's Information Security Policy and also provide for the above mentioned principles. The security thus embedded into the design will be much more effective as compared to putting in security systems as add on components.
- The network design with all the relevant details has to be discussed by the security team and the stakeholders to iron out any gaps. This would be a iterative process till the detailed design plan is finalized.

The security aspects can be incorporated in the design through:

- Access to a the data center LAN/WAN network and its components should be controlled and restricted to only the authorized administrators/users via use of two factor authentication as in
RSA SecurID or RADIUS

- TACACS: Terminal Access Controller Access Control System to provide authentication and authorization while administering the routers, switches etc.
- Using SSL VPN/IPSec VPN for connectivity to provide authentication, integrity and availability
- Encrypted transmission over MPLS or leased lines for confidentiality, integrity and availability
- MAC binding for controlled access.
- Access-list on firewall or routers for controlled flow of traffic.

**Compute Layer Security Considerations**

- The Compute systems include servers with applications that are used by the users. The servers interact with each other and the Storage layer via the network components for their normal functioning. These servers, Windows Unix etc running applications such as mail servers, file servers, web servers, have to be secured both at the Operating system level as well as the application level.
- Design of the compute layer has to imbibe security considerations mentioned in the information security policy. The owners of the various applications and other stakeholders have to take into comply by the requirements specified in the Security policies. Any deviations coming into the deployment has to be taken as an exception with an agreed upon reason.

The security measures that can be taken are:

- Standardization of the Operating system with defined hardening checklist.
- Regular patching of OS and applications through WSUS or SMS client server methods.
- Use of RSA SecurID for authentication and authorization.
- Role based access and password management.
- Putting servers in cluster or load balancing modes for higher availability.
- Backup and Recovery processes

**Storage Layer Security Considerations**

- Storage systems include NAS, SAN, DAS boxes, SharePoint Servers, Tape drives or any other form of data storage system. They interact with the Compute layer via the Network layer to provide the users with the desired information.
- The information security policy should provide guidelines to securing the data stored on the storage systems.
- Availability and performance of the system of the data is a critical factor to be considered while defining the security of the storage system layer as all the data resides on the storage systems.

Some of the ways to secure the data on the storage systems could be:

- Putting storage systems behind firewalls
- Use of encryption mechanisms for encrypting the stored data.
• Controlled access to the storage devices and the residing data.
• Data invisibility to administrators.
• Enforce a strong password policy for all users
• Use Single-Sign-on (e.g., RADIUS) where possible
• Use secure channels for all remote access (VPN, SSL/TLS, SSH, https)

**Security Infrastructure Considerations**

• The security layer includes specific security products as well as the policies and usage of existing components to provide information security. For example the usage of access list in a router/firewall, wherein the system is used to secure the access to critical information.
• The devices and the components should be configured to perform their activities as per the standards defined in the Information Security Policy and the industry best practices.
• The security features available in the components of the other Layers have to made use of in addition to placing specialized security devices.

The basic security infrastructure can consists of

• Antivirus applications
• Web filtering tools
• NAC systems
• Disk/Data encryption applications
• Identify Management and Access Management
• Intrusion Detection Systems or Intrusion Prevention Systems

Regular administration of these security components has to be done to ensure that the systems are updated to cater in any security threat.

The deployment of the above mentioned consideration into the production environment has to be done in a planned manner so as to facilitate the regular tracking of the work and the closure of the activity. It has to be done in coordination with the security team.

**Stage #3 Testing Of Security Implementation**

• Once the Implementation team has communicated that the security implementation is over, the security team has to take charge to review the implementation.
• The review shall be done so as to identify and gaps in the implementation with regards to its mapping with the Information Security Policy.
• The review shall include creation of test scenarios to see the performance of the security system.
• Vulnerability Assessment, Penetration test or other forms of simulation can be used to gauge the performance.
• Gaps found in the implementation shall be reviewed by the security team, the implementers and the stakeholders and the same have to be closed.
- The Testing of the security systems has to be a regular activity in order to keep the security infrastructure prepared for any security threat.

**Stage #4 Daily Operations**

Once the implementation has been completed, the operations have to be handed over to the Operations Teams. To have the security at the desired levels when in operations can be possible only when the people handling the systems are well informed about the security aspects and there are process in place to support their activities.

- Planned reviews of the Information security Policy for catering to the new security threats.
- Defining security processes to support the daily operations of the teams.
- Alignment of support processes such as change management process so as to ensure that the security aspects of the changes are considered prior to going ahead with it.
- External and Internal Audit of the hardware, applications and the processes to ensure their relevance and effectiveness.

**Stage #5 Monitoring Security Status**

The data centers are a dynamic entity that keep changing to provide for the growing business requirements. These changes require significant man hours and tight schedules from the operations teams, and at times can lead to security getting sidelined.

So before the security aspects become a low priority, time consuming daily activity, it is recommended that a dedicated **Security Operations Operations (SOC) Team** be set up to take over the monitoring and management of the security systems.

- The team comprising of dedicate security experts should be responsible for managing the security devices and their monitoring. The team will ensure that the security devices are updated with the latest security signatures and are regularly configured to identify/prevent security threats.
- Dedicated systems such as “**Security Event and Information Management**” system can also be put in the network to provide for a common platform for a centralized monitoring all the security devices.
- The SOC team shall raise security incidents in case an anomaly or non compliance is observed in any of the network components and trace it to closure.

**Stage #6 Incident Management**

The security incidents raised by the SOC team do not carry any relevance if the incidents that its raises are not closed or if the required changes are not made, to close the security gap.
• The closure of a Security Incident has to be time bound with specific SLA for their creation and remediation, depending on the severity and priority of the incident.

• A common knowledge base has to be maintained in order to keep track of frequently occurring incidents and their remediation.

• Changes in the information security can be made in so as to include a scenario of an incident that had some significant effect.

• The incident closures have to be reviewed by the Information Security Manager, Operations Teams and SOC team.

**Stage #7 Additional Security Features**

The data at rest and in motion with the data center can be secured to a good extent by the above mentioned practices.

Still there can be chances where in critical data can be compromised. To avoid such occurrences, a Data Loss Prevention system can be put in place.

• The system keeps track of critical data that is residing in the compute components such as the NAS, SAN, Shared locations, server etc.

• The system can prevent any unauthorized access, sharing or movement of the critical data from these compute components.

• The data flowing in the network such as on mails and chat can also be tracked and stopped.

• Effective Information Security Policy is extremely helpful in making the best use of the Data Loss Prevention system.