UNIT -IV DATA PROTECTION:

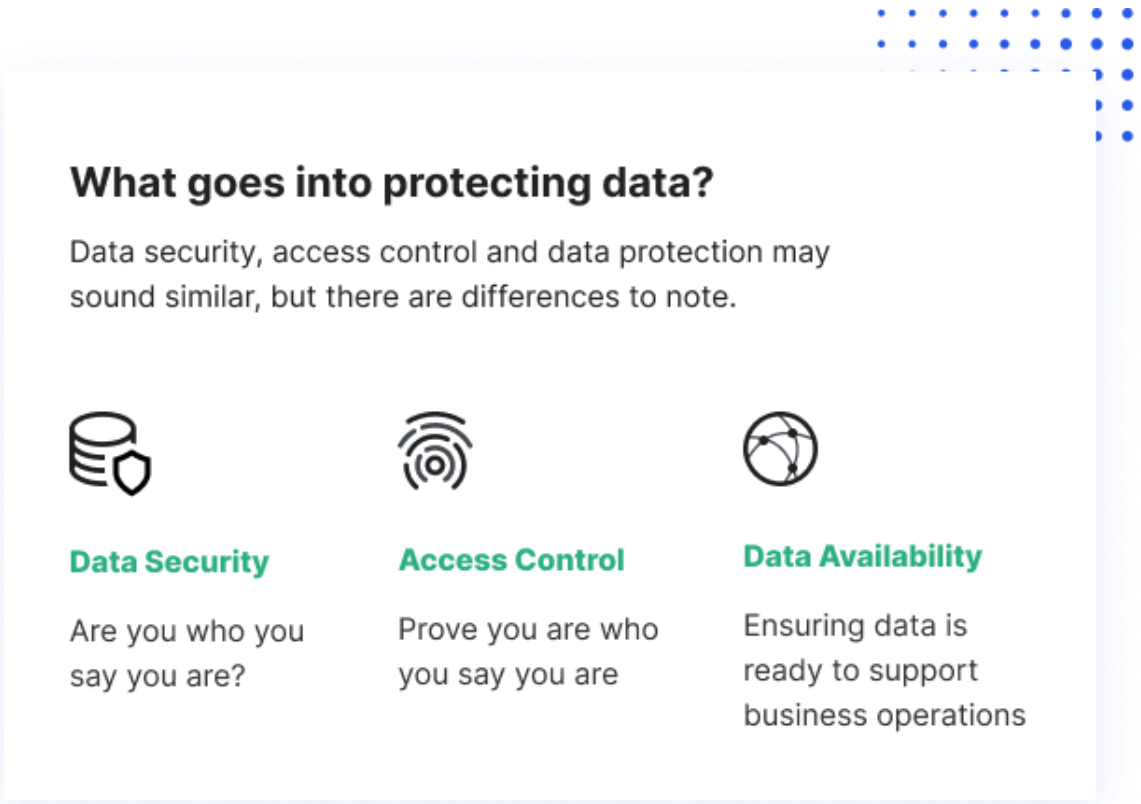
What is Data Protection

Data protection is the process of protecting sensitive information from damage, loss, or corruption.As the amount of data being created and stored has increased at an unprecedented rate, making data protection increasingly important. In addition, business operations increasingly depend on data, and even a short period of downtime or a small amount of data loss can have major consequences on a business.

The implications of a data breach or data loss incident can bring organizations to their knees. Failure to protect data can cause financial losses, loss of reputation and customer trust, and legal liability, considering most organizations today are subject to some data privacy standard or regulation. Data protection is one of the key challenges of digital transformation in organizations of all sizes.

Therefore, most data protection strategies have three key focuses:

- **Data security** – protecting data from malicious or accidental damage
- **Data availability** – Quickly restoring data in the event of damage or loss
- **Access control** – ensuring that data is accessible to those who actually need it, and not to anyone else



Elements of a data protection program

Principles of Data Protection

The basic tenet of data protection is to ensure data stays safe and remains available to its users at all times. These are the two key principles of data protection: data availability and data management.

Data availability ensures users can access the data they need to do business, even if the data is corrupted or lost.

Data management encompasses two main areas of data protection:

- **Data lifecycle management**—automatically distributes important data to online and offline storage, depending on its context and sensitivity. In today's big data environment, this includes methods of identifying valuable data and helping the business derive data from it, by opening it for reporting, analytics, development, and testing.
- **Information lifecycle management**—assesses, classifies, and protects information assets to prevent application and user errors, malware or ransomware attacks, system crashes or malfunctions, and hardware failures.

Enterprise Data Protection Trends

The latest trends in data protection policy and technology include the following:

Hyper-Convergence

With the advent of hyper-converged systems, vendors are introducing devices that can provide backup and recovery in one device that integrates compute, networking, and storage infrastructure. Hyper-converged systems are replacing many devices in the traditional data center, and providing cloud-like capabilities on-premises.

Ransomware Protection

Ransomware is a type of malware that infects a system, encrypts its data, and demands a ransom fee to release it. Traditional backup methods are useful for protecting data from ransomware. However, new types of ransomware are able to infect backup systems as well, rendering them useless. This makes it very difficult to restore the original version of the data.

To solve this problem, new backup solutions are designed to be completely isolated from the corporate network, and use other measures, like data encryption at rest, to prevent ransomware from infecting backups.

Disaster Recovery as a Service

Disaster Recovery as a Service (DRaaS) is a cloud-based solution that allows an organization to create a remote copy of local systems or even an entire data center, and use it to restore operations in case of disaster. DRaaS solutions continuously replicate data from the local data center to provide a low recovery time objective (RTO), meaning they can spring into action within minutes or seconds of a disastrous failure.

Copy Data Management (CDM)

CDM solutions simplify data protection by reducing the number of copies of data stored by the organization. This reduces overhead, maintenance, and storage costs. Through automation and

centralized management, CDM can accelerate development lifecycles and increase the productivity of many business processes.

Data Protection Strategy

Every organization needs a data protection strategy. Here are a few pillars of a robust strategy:

- Audit of Sensitive Data
- Assessing Internal and External Risks
- Defining a Data Protection Policy
- Security Strategy
- Compliance Strategy

Audit of Sensitive Data

Before adopting data protection controls, you must first perform an audit of your data. Identify data sources, data types, and storage infrastructure used throughout the organization.

Classify data into sensitivity levels, and see what data protection measures already exist in the organization, how effective they are, and which can be extended to protect more sensitive data. Often, the biggest potential is in leveraging existing data protection systems that are "lying around" or are not used consistently throughout the organization.

Assessing Internal and External Risks

The security team in the organization should regularly assess security risks that may arise inside and outside the organization. Data protection programs must be designed around these known risks.

Internal risks include errors in IT configuration or security policies, the lack of strong passwords, poor authentication, and user access management, and unrestricted access to storage services or devices. A growing threat is malicious insiders or compromised accounts that have been taken over by threat actors.

External risks include social engineering strategies such as phishing, malware distribution, and attacks on corporate infrastructure such as SQL injection or distributed denial of service (DDoS). These and many most security threats are commonly used by attackers to gain unauthorized access to sensitive data and exfiltrate it.

Defining a Data Protection Policy

Based on the organization's analysis of its data assets, and the most relevant threats, it should develop a data protection policy that determines:

- **The tolerance for risk for every data category**—data protection has a cost, and protection measures must be applied in accordance with the sensitivity of the data.
- **Authorization and authentication policy**—use best practices and historical information to identify which business applications or user accounts should have access to sensitive data.

Security Strategy

With respect to data protection, an organization's security strategy should:

- Take measures to prevent threat actors from accessing sensitive data
- Ensure that security measures do not hurt productivity or prevent employees from accessing data when and where they need it
- Manage backups effectively to prevent ransomware or other threats, and ensure constant data availability

Compliance Strategy

Finally, a data protection strategy must consider compliance obligations. Organizations or specific business units may be subject to a variety of regulations or industry-specific compliance standards. Below are the most significant regulations affecting data protection today.

European Union (EU): the GDPR

The General Data Protection Regulation (GDPR) applies to all organizations that do business with EU citizens, regardless of whether the company is located inside or outside the EU. Failure to comply can result in fines of up to 4% of worldwide sales or 20 million euros. The GDPR protects personal data such as name, ID number, date or address of birth, web analytics data, medical information, and biometric data.

Data protection laws in the USA

The USA does not have a sweeping regulation equivalent to GDPR, but it does have several regulations that affect data protection:

- **The Federal Trade Commission Act** requires organizations to respect consumer privacy and adhere to privacy policies.
- **The Health Insurance Portability and Accountability Act (HIPAA)** regulates the storage, confidentiality, and use of health information.
- **The Gramm Leach Bliley Act (GLBA)** regulates the collection and storage of personal data by financial institutions.
- **The California Consumer Privacy Act (CCPA)** protects the right of California residents to access their personal information, ask for deletion, and request that their personal data will not be collected or resold.

Data protection laws in Australia

The Australian Prudential Regulatory Authority (APRA) introduced a mandatory data privacy regulation called CPS 234 in 2019. CPS 234 requires organizations to improve information security measures to protect personal data from attacks.

CPS 234 applies to accredited deposit-taking institutions (ADI), general insurance companies, life insurance companies, private health insurance organizations, and companies licensed under RSE.

Data Protection Laws and Regulations Report 2022-2023 India (iclg.com)