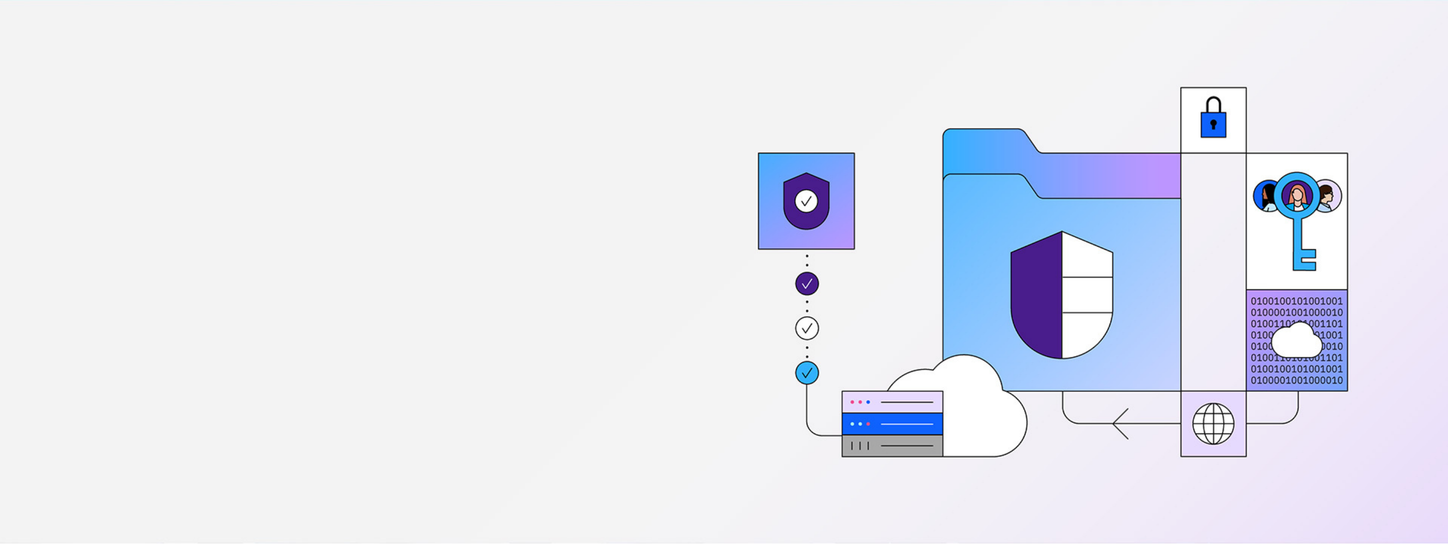
Getting Ready for a New Era of Data Protection: What Your Business Needs to Know

Oct 16, 2023



By Tushar Haralkar

Today, as businesses navigate the disruptions posed by digital transformation, data has become the biggest asset for organizations. However, owing to rampant hybrid cloud adoption, the creation of siloed databases, dependency on the cloud for storage and personal devices, the risks of sensitive data being exposed are also growing multifold.

Further, the Government has introduced the Digital Personal Data Protection Act 2023 (DPDP Act), which marks the dawn of a new era of data protection in India. Data privacy and security are becoming fundamental to the way of business, with high accountability being placed on entities operating in India (data fiduciaries) and how they process the data of Indian citizens (data principals).

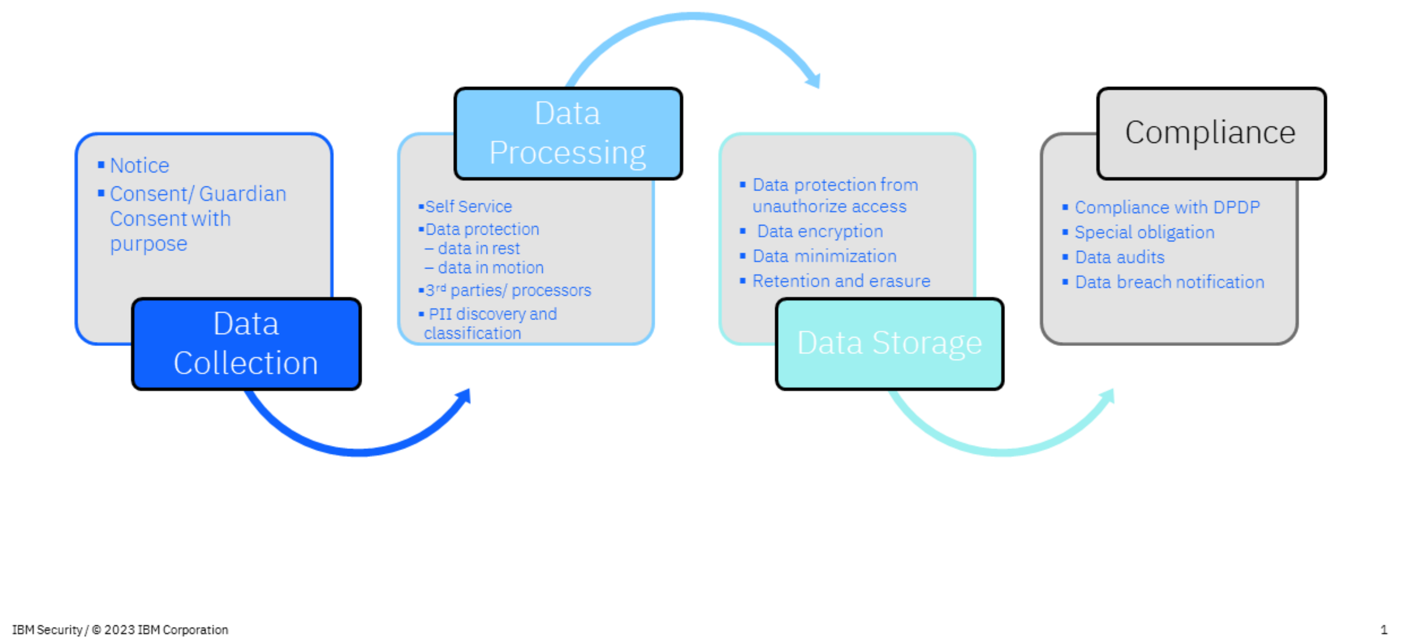
Considering the rapid pace of change in the Indian landscape, you need to reevaluate your data protection mechanisms, ensure the compliance requirements are met and deploy necessary measures to minimize the impact of a data breach.

A simple and effective solution to the above challenges is for your business to **build a robust data-centric cybersecurity program**. The question is, how can you build this program?

Understanding the data lifecycle and defining data protection processes and controls

In today’s digital-first world, your business is collecting data from customers daily. As your customers interact with your products and services through their smart devices, huge volumes of data are being created every minute of the day. This data maybe stored on the cloud or on-premises, and then used and analyzed via technologies such as AI for critical decision-making. Therefore, it is important for your business to understand the lifecycle of such data and how it evolves over the course of its journey, to be able to implement robust data privacy and data security mechanisms.

Keeping the DPDP Act 2023 in mind, the below chart is a representation of the aspects you need to take into consideration when progressing through each of these stages.



Data Collection

- Notice
- Consent/ Guardian Consent with purpose

Data Processing

- Self Service
- Data protection
  - data in rest
  - data in motion
- 3rd parties/ processors
- PII discovery and classification

Data Storage

- Data protection from unauthorize access
- Data encryption
- Data minimization
- Retention and erasure

Compliance

- Compliance with DPDP
- Special obligation
- Data audits
- Data breach notification

IBM Security / © 2023 IBM Corporation 1

Data in the Cloud

According to a recent report from Ernst & Young, about 80% of Indian businesses are implementing cloud strategies for modernizing the technology stack and infusing intelligence into business applications. With the growing dependency on multiple clouds, enterprises are struggling to protect their structured and unstructured data that are multiplying across public clouds, data warehouses, and popular SaaS apps. This has also made the average company’s digital footprint and attack surface larger, increasing the possibility of breach of sensitive data.

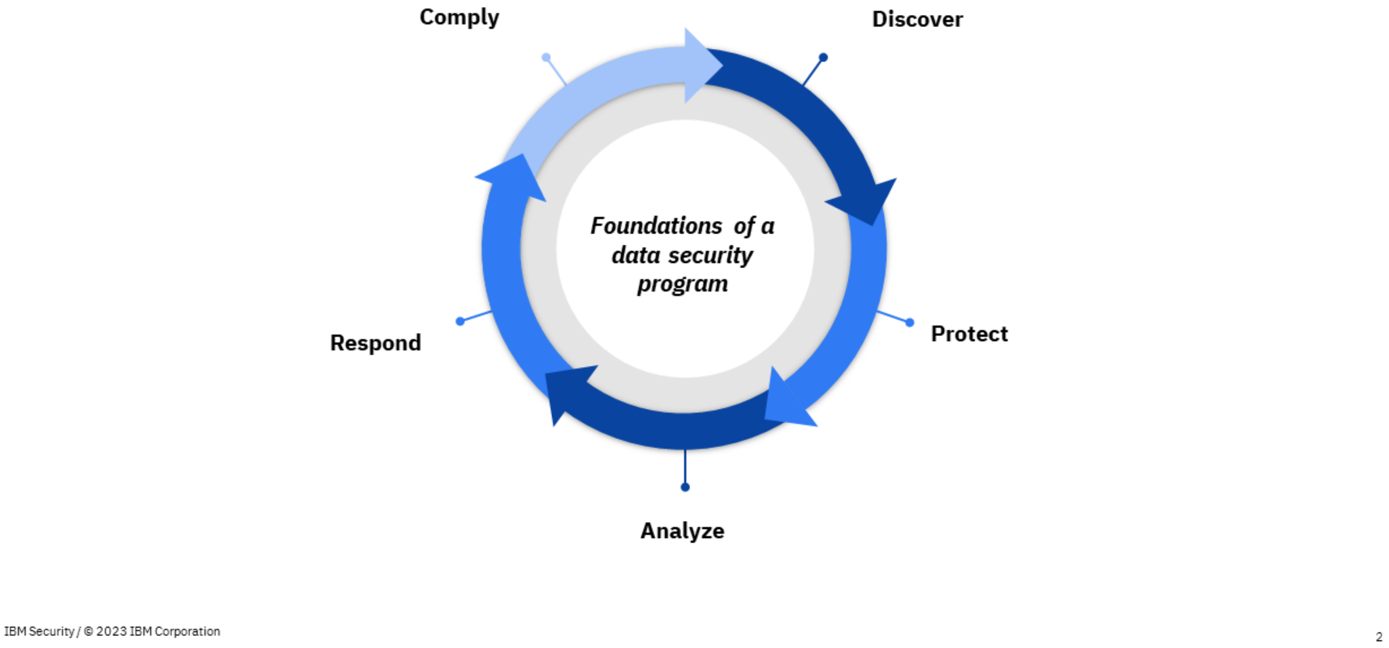
Tackling Shadow Data

As more data is being collected, businesses are being increasingly blinded by such data. They don’t know what data is being collected and where such data is stored, which makes protecting such data a huge challenge. In fact, a report from Gartner revealed that globally businesses are drowning in data – only 15% of data collected is viewed as business-critical data. About 33% is viewed as Redundant, Obsolete and Trivial Data (ROT Data) and the remaining becomes dark data, which only adds to a business’ risk exposure.

We must acknowledge the new reality is that data is everywhere, and security is not.

Immediate Steps Your Business can Take

Here are 5 quick steps that your business can consider to build a robust data security framework and protect data across the cloud.


Comply
Discover
Foundations of a data security program
Protect
Respond
Analyze
IBM Security / © 2023 IBM Corporation
2

- **Discover:** Uncover and categorize your sensitive data throughout both on-premises and cloud-based data repositories. This is a crucial first step toward defining proper security policies for different data depending on its criticality and compliance requirements.
- **Protect:** Safeguard sensitive data by implementing policies and actively monitoring data activities.
- **Analyze:** Utilize advanced analytics and assessments to thoroughly analyze and fortify defenses against risks and vulnerabilities.
- **Respond:** Take immediate action against threats and dispatch actionable alerts to security operations systems in real-time.
- **Comply**: Adhere to data privacy and security regulations while streamlining the process of auditing and reporting.

IBM believes that the future of security is an **open, connected platform approach** - leveraging open standards, AI and automation to connect security tools and data across the hybrid cloud.

Towards this, **IBM Security Guardium** is a modern, scalable data security platform that is ready to meet the demands of today's progressing environments. It helps discover where sensitive data lives, encrypt and monitor what's important and reduce your risk, protect sensitive and regulated data across multiple cloud environments, and respond in real-time to threats, while managing compliance obligations.

Further, businesses can use Comprehensive Cloud Security Posture Management (CSPM) to apply cloud security best practices to complex cloud environments. CSPM can visualize asset inventories, network interconnections and access pathways to important data. CSPM also enables risk visualization, incident response and DevOps integration. It can map risks to compliance standards and best practices.

The Indian cybersecurity ecosystem is at a tipping point. With emphasis being placed on personal data protection like never before, it is imperative for organizations to understand their data lifecycle and ensure there are clearly defined processes and control mechanisms in place when collecting, analysing, storing or sharing such data on-prem or on the cloud. Businesses must adopt robust data security programs that can help them discover and protect their data, proactively analyse and respond to potential threats, and ensure compliance with emerging regulations. Time is of the essence and your business needs to act now.

To understand how you can build a robust data security program with IBM’s solutions, visit our website to book a free consultation with our team of experts.

Tushar Haralkar is Principal Technical Sales Leader - Security Software, IBM India and South Asia.

Blog Categories

Secure