Data Security

AT THE SPEED OF BUSINESS

Shobhit Kumar,
Senior Director, Industrials, Tredence Inc.

Table of Contents

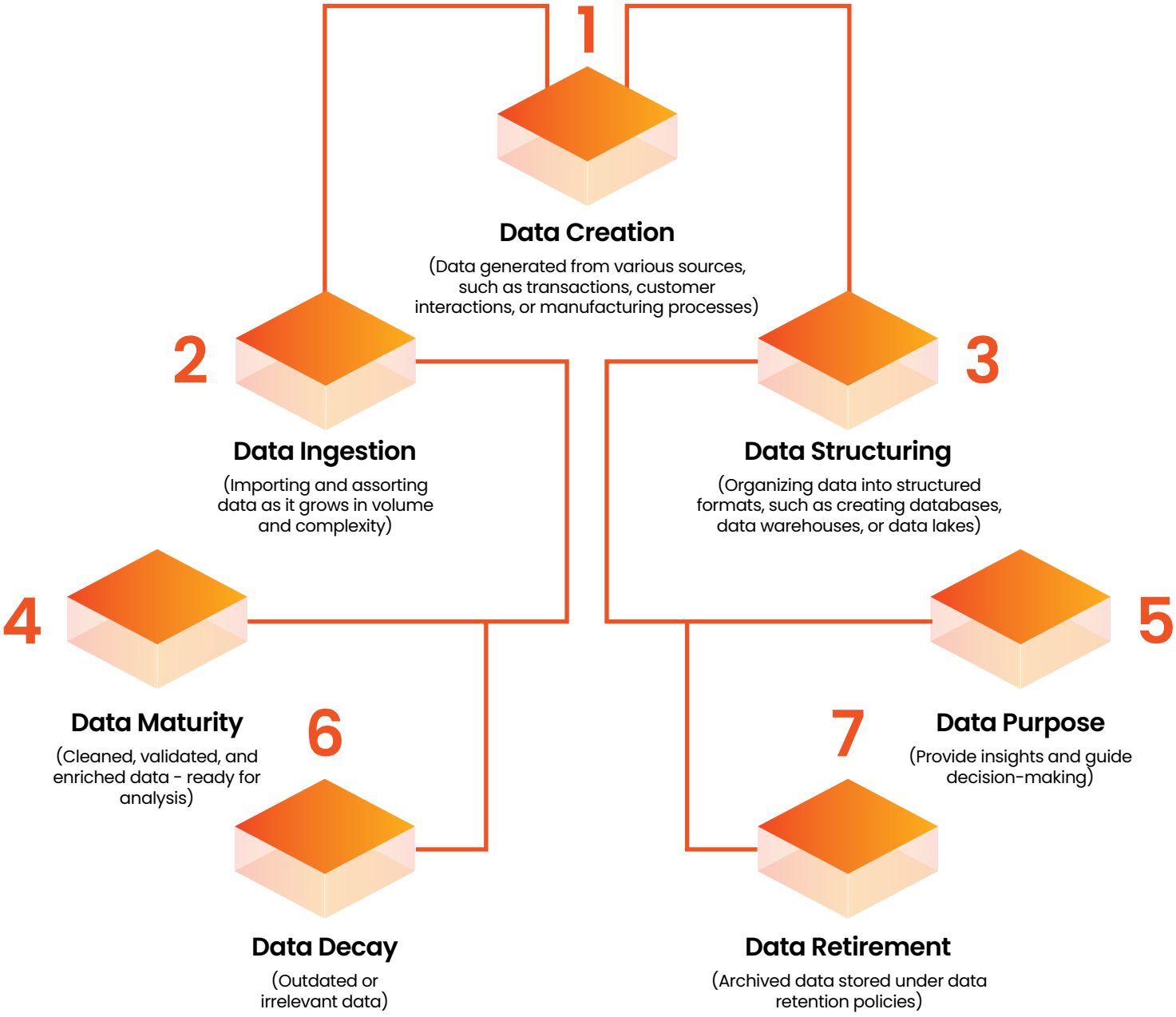
© Copyright 2023. Tredence.Inc. All Rights Reserved

Data is a peculiar thing. Peculiar because it can make or break an organization.

When tamed, it gives invaluable insights; it becomes challenging to decipher when left wild. When safeguarded, it is precious; when not, it can topple years of hard work.

But if we talk in more relatable semantics, data is a 'peculiar living entity.' It is born, grows, matures, has its purpose (may or may not serve it), decays, and retires. It is meaningful when structured and more meaningful when it mimics a pattern.

This requires tailored security measures at each stage of the data life cycle.



The one who understands the data life cycle can harness its full potential.

© Copyright 2023. Tredence.Inc. All Rights Reserved

Unlocking ROI Across the Data Lifecycle

Like Rubik's cube, the RoI of data security investments shifts and moves at every stage of the data lifecycle. There is more than one permutation to it. So, recognizing that the ROI of data security investments changes throughout the data lifecycle is vital.

Each stage—from creation and storage to processing and eventual retirement—necessitates customized security measures.

Data Creation:
Laying the Groundwork of Security

When data is created or generated, active and passive, through users, businesses, transactions, sensors, cookies, browsing history, and more, it is critical to implement authentication and access controls to ensure authorized access. For example, we can categorize data based on sensitivity by deploying data classification policies.

Early investment is rather crucial to ensure data is vaulted and only authorized personnel has its key.

Data Ingestion:
The Critical Focus

Data security takes center stage as data progresses to the ingestion phase. The ROI at this stage increases, accompanied by a higher data security cost.

Enterprises must prioritize implementing and maintaining proper security measures through encryption and secure data storage techniques.

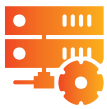
A Deloitte survey found that 40% of organizations consider data encryption as their primary method of protecting data. However, with proper data ingestion security measures, enterprises can significantly reduce the risk of data breaches.

© Copyright 2023. Tredence.Inc. All Rights Reserved

Data Structuring:
The Foundation of Secure Data Management

Data structuring involves data modeling, and metadata management, which forms the foundation for data usage, management, and security. With robust data structuring and classification, granular data security measures can be taken, limiting and adding extra layers to the sensitive data.

Therefore, organizations should be proactive in their investments at the data structuring stage to advance security measures and promote better analysis of data.



Data Maturity:
More Value Over Time

Data maturity is the net summation of how advanced an enterprise's data processes are, reflecting its data management capabilities, from data acquisition to analysis, and how good the insights are. As the volume and complexity of data rise, there has to be an evolving data security process that keeps upgrading data management practices, improving the data quality.

To ensure that mature data's integrity is preserved, enterprises must implement stringent security measures at each stage of its maturity, which can result in effective data utilization, better experiences, and an advantage over competitors. It's more of a strategic move to invest in matured data security.

Data Purpose:
Harnessing the Strategic Objective

By intentionally applying data in alignment with an organization's strategic goals, it directs data collection and management efforts, ensuring resources are not misused on irrelevant data rather than assisting in developing various security measures for multiple data types. By aligning data purpose with strategic objectives, organizations can maximize the value of their data, facilitate informed decision-making, and achieve their objectives. It is a crucial stage in the data lifecycle that can considerably increase ROI.

Data Retirement:
The Final Stage

The final phase of the data lifecycle, data retirement, entails securely archiving or discarding obsolete data. Retiring data, especially redundant, outdated, or trivial (ROT), improve data management efficiency and reduces storage costs. Effective data retirement reduces legal risks associated with data retention and improves data quality by removing redundant data, thereby releasing additional Return on Investment (ROI) from data lifecycle management practices.

© Copyright 2023. Tredence.Inc. All Rights Reserved

Three States of Data: Trifold Challenge for Organizations

Data exists in three states – at rest, in motion, and in use – each with its own peculiar need for security. Each state corresponds to the data life cycle stages:

1. **Data transfers from its source to a storage location during data creation and ingestion.**
2. **It is organized for effective use and at rest during the structuring phase.**
3. **It can exist in any maturity and purpose-related state, including storage, transmission, and processing.**
4. **Obsolete data remains at rest during degradation and is securely archived during retirement.**

Recognizing these connections ensures appropriate security measures are implemented at each stage of the data's life cycle, providing comprehensive data protection.

Data at rest

Data in a data warehouse, transactional database or any other type of data store becomes vulnerable to data theft. And as it is at rest, all a malicious actor want is an access point. And if it happens, the entire security infrastructure could crumble, muddying your stakeholder's faith in you.

© Copyright 2023. Tredence.Inc. All Rights Reserved

Data in motion

When the data is open to be accessed over the web or an organization's internal networks, it is quite defenseless. Therefore, you need a barrier that holds strong and, thankfully, detailed cloud security posture management (CSPM) and robust network security implementation coupled with compliance/privacy laws like GDPR, HIPAA, CCPA etc. necessitate safeguarding such data.

The secure transmission of data during its transition from one state to another is another essential aspect of data security. If data can be manipulated or altered during transmission, it can significantly affect the ultimate outcomes and decisions based on that data. Therefore, secure data transmission protocols, encryption, and authentication mechanisms are necessary to protect data integrity in transit.

Data in use

Now, there's this final data that is currently being used by you, your peers, stakeholders, or your organization. It is not static; rather, it's dynamic, continuously transforming – it's being created, retrieved, deleted, updated, or just siloed temporarily, awaiting change. Because of its differentiated nature, it is more susceptible to theft or manipulation. And its security equally depends on the person that uses it and the infrastructure that it stays in. Therefore, persona -based access control ensures only authorized personnel can access the information.

© Copyright 2023. Tredence.Inc. All Rights Reserved

Incorporating Security-By-Design Approach

Organizations must consider incorporating security into system design to address these challenges and embed security throughout the data lifecycle. For example, instead of regarding data security as an addendum or an add-on, it should be fundamental to the overarching enterprise data governance framework.

By infusing data security into the data governance framework, organizations can implement robust security measures at each data lifecycle stage, proactively identifying potential vulnerabilities and implementing the necessary data protection measures.

Furthermore, incorporating security into system design also helps address the problem of data bias. Data bias can substantially impact the caliber of decisions. For example, the models and forecasts may be inaccurate or biased if a dataset is prejudiced against a particular demographic or lacks diversity. As a result, organizations can ensure more accurate and equitable decision-making by designing systems with built-in checks and balances to identify and mitigate data bias.

The Impact of Data Bias on Enterprises

When interjected deliberately or by mistake, data bias in AI/ML models and other forms of analytics can obfuscate the enterprise security view. Remember that the crux of your data is its precision; any bias erodes its veracity, diminishing the quality and efficacy of your insights and conclusions. High-quality data is the foundation of comprehensive data security, not just the foundation of good analytics. A deterioration in data quality could render your security systems vulnerable; ineffective access controls and misidentifying security threats could become a reality.

No shortcuts exist in the battle for secure and sensible decision-making: Organisations must confront and remove bias to ensure their data quality is of the highest standard, strengthening their security measures.

© Copyright 2023. Tredence.Inc. All Rights Reserved

Yet, not only internal processes influence data bias; external forces, such as the media and popular culture, also play a role. For example, diverse on-screen characters can shape societal attitudes and imperceptibly affect the generation and collection of data. As a result, organizations must remain cognizant of these effects, work persistently to eliminate bias, and develop inclusive, diverse datasets to combat this. Ultimately, our data should reflect the world we desire, not the world as it was.

Cloud Security:
A Shared Responsibility for E2E Enterprise Data Protection

Since the cloud is essential to any enterprise's IT landscape nowadays, IT, InfoSec, and Application development teams need to put their heads together to ensure that they don't leave everything to the hyperscalers like AWS, Azure, or GCP to manage. As a good thumb rule, a cloud provider should be responsible for the security of the cloud (like secured storage, compute resources, infrastructure assets, etc.). In contrast, security in the cloud (like data, application, identity management, firewall setup, etc.) should be the enterprises' responsibility by effectively using cloud infrastructure and services.

Bottom line:
Data Security is an Unending Journey that Requires Vigilance, Adaptation, and Continous Improvement

The peculiar, ever-changing nature of data makes it both an asset and a challenge for any organization. When seen through the lens of its lifecycle, its potential and vulnerability are apparent at each stage, from creation to retirement. Understanding this lifecycle enables organizations to implement security measures that ensure the integrity, accessibility, and relevance of the data. Further, throughout the data lifecycle, the ROI of data security investments is not static but rather keeps shifting. Moreover, assuring the security of data at rest, in motion, and in use is about more than just compliance; it's also about maintaining the confidence of stakeholders and customers. In addition, the importance of data bias in enterprise security cannot be overstated, nor can its impact. As a result, it is crucial to incorporate security into system design in order to reduce bias and promote accurate and fair decision-making. Similarly, in an era where the cloud has become an integral part of IT infrastructure, the responsibility for security should be shared between cloud providers and enterprises, with cloud providers safeguarding the cloud and enterprises securing what is in the cloud.

In a nutshell, data security is not a destination but rather an ongoing journey of vigilance, adaptation, and improvement. It necessitates an initiative-driven approach, a shared sense of responsibility, and a commitment to maintaining stakeholder confidence at all costs. When managed effectively, the benefits are substantial: enhanced decision-making, decreased risk, and increased stakeholder confidence.

© Copyright 2023. Tredence.Inc. All Rights Reserved

About the Author

Shobhit Kumar,
Senior Director, Industrials,
Tredence Inc.

Shobhit is a seasoned professional with experience in CXO-level client stakeholder management, multi-practice program governance, delivery management, delivery KPIs ownership, cost management, people management, consulting, practice building, program management in IoT, data science, machine learning, analytics, business insight, and information management.

Shobhit's domain experience includes healthcare payer, provider, manufacturing, and financial services. He is also an expert in data science, data quality, and master data management.

DEVELOP AND DELIVER YOUR DATA SECURITY WITH EXPERT'S HELP:

Let's get started →

Name:

Email:

Drop a note here:

For more information please visit www.tredence.com

© Copyright 2023. Tredence.Inc. All Rights Reserved