Managing Data Protection Challenges in the Era of Digital Business

Dr.G. Arasuraja, Associate Professor, St. Joseph's Institute of Technology, Chennai, Tamil Nadu India.

arasurajag@stjosephstechnology.ac.in

Introduction

Data has now become one of the most important assets of any business today. It is the constant flow of customer data, transaction data, intellectual property, employee data, and operational analytics, which help businesses to make decisions, understand customers better, and innovate. However, the problem is that data becomes very difficult to manage. As businesses produce more and more data in the form of information within their digital environments, the protection of this data has now become one of the most important issues that businesses face.

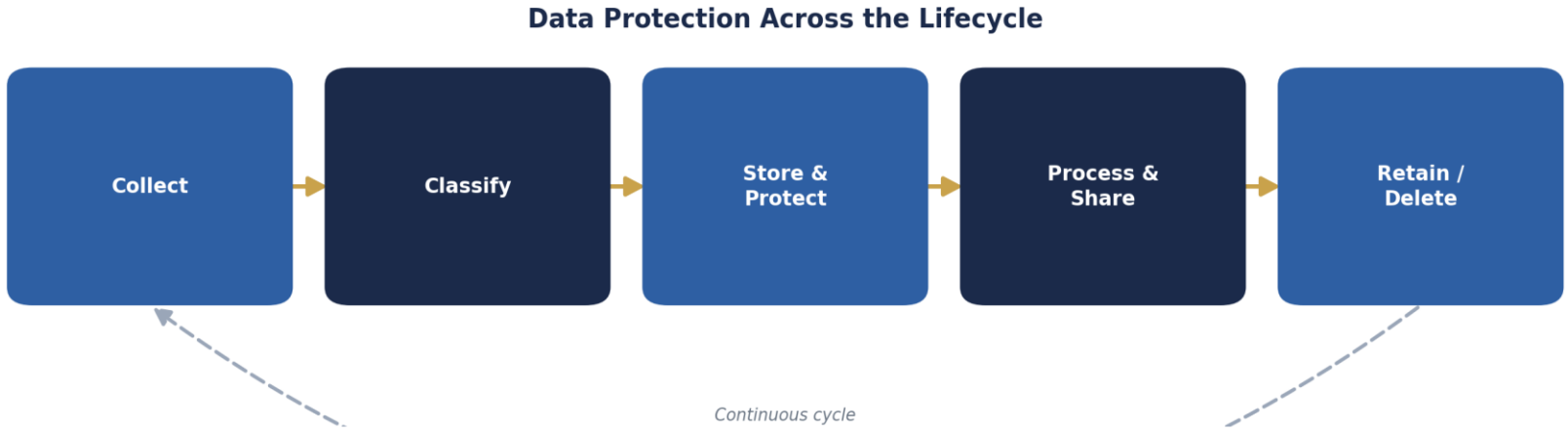

Figure 1: Process overview

Figure 1 showing the lifecycle of continuous data protection, which includes data gathering, classification, storage, protection, processing and distribution, and retention or destruction.

This paper will discuss the major issues of data protection that organizations face today, the legal environment that determines their data protection obligations, and possible solutions for addressing these issues.

The Expanding Scope of Data Protection

Expanding Nature of Data Protection

Data protection was initially all about ensuring the safety of structured data stored in centralized databases. In today's world, however, the ambit of data protection has increased drastically. Companies have started managing their data on cloud computing, software-as-a-service applications, mobile phones, Internet of Things, systems of third-party vendors, and artificial intelligence/machine learning workflows handling huge amounts of data.

These developments present a number of challenges:

Data sprawl with the spread of data over many systems and platforms, usually without any central management or oversight, companies often find themselves in the dark about the exact nature and whereabouts of the data that they have, and which individuals are accessing the data.

Shadow IT and Shadow Data By using unsanctioned software and storage options in order to get things done, employees may end up creating isolated areas of sensitive data outside of the company's knowledge and purview.

Third party/vendor risks the use of third parties by modern organizations means that more avenues are created through which sensitive information could leak. In such instances, the security measures of these third parties should not be weaker than those of the organization.

Cross border data transfer Businesses that operate internationally tend to move data across borders. This is complicated further by the fact that different jurisdictions have different regulations with respect to international data transfer.

The Regulatory Landscape

The issues of data protection have been made even more complex by the changing nature of the regulatory environment worldwide. In the past decade, there has been the emergence of a whole lot of data protection and privacy legislations that apply their own sets of unique rules.

These legislations have included the EU's GDPR which set very high standards for consent mechanisms, data subject rights, breach notifications, data transfers, and financial penalties for any kind of non-compliance. In the years after that, many other jurisdictions have followed suit by introducing similar legislation that includes industry and state-level legislations within jurisdictions and data protection laws at the national level, with the example of India's Digital Personal Data Protection Act.

All these different legislations make it very difficult for businesses operating in several jurisdictions to ensure compliance because some of the requirements in the areas of

consent mechanisms, data subject rights, breach notification period, data localization, and uses of the data may be very different from jurisdiction to jurisdiction.

There are heavy penalties for non-compliance in addition to reputation risks.

Core Data Protection Challenges

Achieving the Balance between Accessibility and Security

Data must be accessible for companies to operate properly and make decisions, but if too much data is accessible, it raises the chances of either unauthorized access or data exposure. The challenge here lies in the ability to strike the correct balance and develop appropriate access control policy built around the least privilege principle, which states that data access should be provided solely for the purpose of the individual's work.

Classification and Management of Data

Another challenge in data protection is that many firms find it difficult to classify the data properly. Since classification is a prerequisite for developing proper data protection strategy, failing to do it right means that the organization will not know how to protect its data and in what way. To solve the problem, one needs to build the proper data governance framework.

Data Protection During its Entire Lifecycle

For proper data protection, it is important to protect data during all stages of its lifecycle, starting from creation and collecting, then storing, processing and sharing it until data is archived and deleted. Each stage requires certain security actions to be taken.

Data Protection on Clouds and Hybrids

As organizations transition to clouds and hybrids, perimeter-based solutions fail to protect their data effectively. Data can be exposed by improper cloud storage configurations, overly permissive policies for accessing information, and a lack of clarity about what each party is responsible for as part of the shared responsibility model. The use of cloud data protection tools and an understanding of the shared responsibility model are necessary conditions for protecting data.

Insider Risk Management

It is not true that all the data protection problems faced by organizations come from outside. Insider threats are a very important aspect of data protection that is often underestimated by companies. To ensure the security of data, an organization should monitor suspicious behavior related to data access, remove access as soon as possible after employees leave the company, and have acceptable policies for data usage.

Responding to Data Breaches

Data breaches continue to pose a threat despite best intentions. In addition to being ready for data breaches and containment, companies should know how to handle the difficult task of notifying the right people according to a specific timeframe. This includes, among other things, informing those who were victims of the data breach, regulatory bodies, and at times even business partners. It goes without saying that a properly crafted breach response strategy is crucial in handling breaches.

Strategies for Effective Data Protection

For organizations attempting to address these challenges, a multi-level strategy is warranted.

Data discovery and mapping. Knowing the extent of data, its location, and how it travels through the organization are the first and foremost steps toward protection. There are tools that allow organizations to discover and map their data automatically in order to keep track of the volume and location of it.

Encryption and tokenization. It is crucial to encrypt all sensitive data not only at rest but also when being transmitted and use tokenization for extremely sensitive data like payment information. This will lessen the consequences of unauthorized access due to the impossibility of using encrypted data without the decryption key.

Access control and identity management. Role-based access control and multi-factor authentication will help in making sure that access to the data will be maintained over time regardless of organizational changes.

Tools for preventing data loss. Data loss prevention tools help to detect any unauthorized efforts to transfer information outside the established parameters via emails, file transfers, and removable media. This is essential in mitigating the risks associated with both unintentional and deliberate data leaks.

Privacy by design. Implementing privacy and data security concerns in the development of new software and systems is much more efficient than trying to incorporate those concerns into existing systems.

Vendor risk management. Vendor risk management includes conducting due diligence procedures for all third-party providers in order to ensure that data protection procedures are extended beyond the perimeter of the organization.

Routine auditing and assessments. Routine audits of the data protection policies, including penetration testing, compliance assessments, and privacy impact assessments, help to identify and close the vulnerabilities within the system.

Conclusion

Protection of data in the age of digital business is a much more complex issue than that of mere information security. In

order to achieve this aim, companies should face an increasingly complicated environment of regulations, deal with data in complex digital environments, reconcile conflicting requirements for data availability and security, and be ready for security issues that cannot be avoided anymore. Companies that are able to treat data protection as a strategic issue, taking into account adequate governance, technical measures, and corporate accountability, will be much more likely to safeguard their most valuable asset in the digital age.