The Indian Journal for Research in Law and Management
Open Access Law Journal – Copyright © 2024
Editor-in-Chief – Prof. (Dr.) Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

The term data protection is used to protect the content and procedure which is followed to safeguard the interest, privacy of data and the process of protecting the sensitive information from loss or damage.Cyber security refers to the protection which is taken against cyber threats like hacking, stalking etc.This blog explores the vital concepts of data protection and cybersecurity, aiming to take necessary measures to safeguard the digital platform. While data protection sets the stage, cybersecurity takes center stage in defending against digital threats.It is required to ensure the people of business entities, government organisations that they feel safe about their data which is saved that they will not suffer any loss regarding it. Data protection means to safe the data before people suffer. For ex: Apple has claimed to have the best data protection security and it does not allow any sort of excessive websites or apps which can breach the privacy of its consumers and also prevents hackers. In the present times, cyber related crimes are highly increasing due to which it is required to make stringent laws regarding it and things which could help to protect it. Data protection and cybersecurity are inseparable components of resilient digital infrastructure. There should be data encrypting which means that there should be a process which will ensure that the data remains unreadable even if there occurs an unauthorised access. Implementing these things ensures that data is protected both in transit and at rest also. Also people should be educated more regarding this concern so that they can recognize any risk which can occur by giving them training progams or by providing them sessions regarding this. Due to cyber crime , cyber threats are also increasing because their data gets leaked. There should be regular audits and updates which would help to identify vulnerabilities and weakness in the system. Keeping the system and software updated ensures that known vulnerabilites are patched. Data Protection Trends

“Here are some important trends driving the evolution of data protection.

Data Portability and Data Sovereignty

Data portability is an important requirement for many modern IT organizations. It means the ability to move data between different environments and software applications. Very often,

data portability means the ability to move data between on-premises data centers and the public cloud, and between different cloud providers.

Data portability also has legal implications—when data is stored in different countries, it is subject to different laws and regulations. This is known as data sovereignty.

Traditionally, data was not portable and it required huge efforts to migrate large datasets to another environment. Cloud data migration was also extremely difficult, in the early days of cloud computing. New technical methods are developing to make migration easier, and thus make data more portable.

A related issue is portability of data within clouds. Cloud service providers tend to have proprietary data formats, templates, and storage engines. This makes it difficult to move data from one cloud to another, and creates vendor lock in. Increasingly, organizations are looking for standardized ways of storing and managing data, to make it portable across clouds."[1]

One such incident which shocked the world crazy is the data leak of the pegasus airlines.

"In June 2022, Pegasus Airlines discovered an error in the configuration of one of their databases. It turned out that an airline employee misconfigured security settings and exposed 6.5 terabytes of the company's valuable data.

As a result of improper configuration of an AWS bucket, 23 million files with flight charts, navigation materials, and the crew's personal information were available for the public to see and modify.

What can we learn from this data leak?

To ensure that your employees don't make similar mistakes, make sure to conduct regular cybersecurity training as well as to establish security policies in your company. Ensure that employees working with database configurations know the right way to configure databases and are aware of best practices to avoid data exposure.

Regular security audits can help your organization timely identify and address misconfigurations or vulnerabilities in databases and systems. By regularly auditing the

[1] Cloudian, What is Data Protection and Privacy (Last Visited:21-01-2024);https://cloudian.com/guides/data-protection/data-protection-and-privacy-7-ways-to-protect-user-data/

security of your infrastructure, you can prevent security gaps or employees ’mistakes from being exploited by malicious actors.

Enabling user activity monitoring on AWS can also help you promptly identify and respond to suspicious events, reducing the risk of critical data being stolen from your cloud environments.”[2]

In conclusion the relation between cybersecurity and data protection is being highlighted with the proper explanation of the said terms with specific conditions and examples provided. There are counter measures specified for the enhancement of the data protection with the data leak of the pegasus airline case.

[2] Ekran,Top 10 Best-Known Cybersecurity Incidents and What to Learn from Them Aug 23 (Last Visited: 21-01-24); https://www.ekransystem.com/en/blog/top-10-cyber-security-breaches