# Data Security and Protection

*Geetha A. J.* [1]

## Abstract

**Greater the dependency on computers and other digital devices, greater is the potential risk of data theft and loss. Databases are one of the important valuable assets of any organisation. The present paper analyzes the concept of data protection, breach of data security, significance of data protection, and ways to safeguarding the data. The protection laws prevailing in India and need of implementing a comprehensive legal backup is discussed in the present paper.**

***Keywords :*** **Data security, safeguarding**

## I. INTRODUCTION

As internet usage has increased exponentially, so has the importance of data privacy and protection. Websites, applications, and social media platforms commonly need to collect and reserve personal data about users in order to provide services. However, some digital platforms on the other hand may violate data collection and usage standards, leaving users' data with less privacy. This also increases threat from criminals who steal data for fraudulent acts.

'Data security is the practice of preventing unauthorised access, unintentional loss, disclosure, alteration, manipulation, or corruption of digital information across its entire lifespan, from creation to destruction' [1]. Protecting the data is crucial for safeguarding personal and organisational information that is confidential.

There are two kinds of threats for data security. Insider threats and third-party threats are the two major perils which can challenge the data security and privacy.

⇳ **Internal Threats:** Internal threats to data security may arise from insiders or third party. Insiders with evil intent may take advantage of their lawful access credentials to destroy or alter sensitive data for profit or to satisfy their personal vendettas. Friends, neighbours, current or past employees, third-party collaborators, or contractors can all make threats [1].

Insider dangers that are unintentional are no less harmful. An unintended click on a link in an email could compromise a user's credentials or release malware on corporate systems and that can damage a whole lot of protected information. A simple negligence or carelessness on the part of the end user can also result in accidental exposure of confidential or private data. An employee of the company might email confidential information to the wrong person or upload it to an unprotected network [1].

Any risk posed to an organisation by third parties in its operation or supply network is referred as third-party threat. Such persons include partners, contractors, retailers, suppliers, or service providers or anybody who have access to internal business or customer data, systems, processes, or other sensitive information [1].

⇳ **External Threats:** External threats may come from hackers. These hackers are brilliant coders who know how data is stored and used in a company system. Hackers work hard enough to find a way to get into any system. Web jacking, Logic bombs, Phishing, and DoS attackers are few of the tactics used by hackers to get access to protected system and networks. Any company or organisation which uses customers personal information

Paper Submission Date : July 10, 2023 ; Paper sent back for Revision : July 20, 2023 ; Paper Acceptance Date : July 25, 2023 ; Paper Published Online : October 5, 2023.

[1] Geetha A. J., *Assistant Professor*, Department of Journalism and Mass Communication, Sri Dharmasthala Manjunatheshwara College (Autonomous) Ujire - 574 240, Karnataka. Email: geethabilinele@sdmcujire.in ; ORCID iD : https://orcid.org/0009-0007-3337-573X

**DOI : https://doi.org/10.17010/ijcs/2023/v8/i5/173323**

must have a good cyber security system and must be able to address violations of cyber security effectively [2].

## II. SIGNIFICANCE OF DATA PRIVACY

If the internal threats and third party threats pose a significant loss to an organisation, there should be a proper policy and method to protect sensitive data. Because of this, data security is quite beneficial.

➥ **Information Protection:** Sensitive information should never be leaked. Whether it is a bank's customer list or a security agency's employees list and information, these are delicate secrets that should not be made public. All of this information can be protected if the data privacy is effectively implemented [2].

➥ **Reputation building:** Any organisation that can retain confidentiality of its employees and customer's data helps to build confidence among all stakeholders, including clients who are sure that their personal and financial data is protected [2].

➥ **Marketing and competitive advantage:** Safeguarding sensitive and confidential information from unauthorised access and disclosure offers marketing and competitive advantage. To preserve one's competitive advantage, any access to future development or expansion plans must be highly limited.

➥ **Reduces development and maintenance expenses:** The sooner the company includes security measures into its policy guidelines and operations, the less money they have to spend on retrieving the data and modifying the code [2].

## III. SAFEGUARDING THE DATA

Most cyber security experts advise taking into account the following tools and approaches to secure personal and financial data:

**1) Access control**: The guidelines to limit who may access, edit, store, and share data is the foundation of data security, regardless of its location [4].

➥ Controlling, restricting, and monitoring the access levels of employees for data and changing them as and when required [5].

➥ Changing the passwords regularly and do so right away when an employee leaves.

**2) Data backup:** The best advise is that prevention is better than cure. Keeping the data backup acts as a protection policy in the case the data is corrupted, deleted, or stolen, as may occur in the event of a malware attack [4].

**3) Encryption of data:** If access control is the first step of a data security policy, encryption is its final step. According to experts, it should not be negotiable for sensitive data, whether in use or not, or in transit. Encryption makes the contents of a sensitive file unreadable if access control fails and an unauthorized person tries to utilize it [4].

**4) Data masking:** Masking the data is an intelligent move to protect the data. Data masking makes data encryption by substituting crucial digital information with fictitious data. This is helpful if an organization needs to share a non-confidential version of data with certain users for reasons such as database administration, research and development, software testing and user training [4, 5].

**5) Security of databases:** An organization's databases should be as secure as a bank vault. The cyber security professionals highlight the recommended practices for ensuring database security, such as performing routine access checks and monitoring database activity [4].

**6) Data Loss Protection:** Data loss protection prevention can prevent a user from transmitting or downloading a protected file. DLP can prevent unauthorised access and alert cyber security personnel to violations and suspicious activities [4,5].

**7) Instruction on security awareness:** One of the biggest risks to data security is deliberate or unintentional mistakes inside or third party stakeholders of a company. Therefore, it is important to provide security training to make them aware of organisational security rules and data assaults [4].

No matter how large or small an organisation is, or what type of information the organisation exchanges, data security must be prioritised. It is an essential component that keeps the company and personal data flowing efficiently and aids in the preservation of all key information.

## IV. DATA PROTECTION LAWS IN INDIA

There is no specialised cyber security law in India [7]. The Information Technology Act of 2000 (the IT Act) and the rules and regulations enacted under it address cyber security and cybercrime [7]. The IT Act not only identifies and protects electronic platform transactions, but it also includes rules targeted at preserving electronic data, information, or records and prohibiting unauthorised or criminal use of a computer system. Some of the cyber security offences specifically foreseen and punishable under the IT Act include hacking, denial-of-service attacks, phishing, virus attacks, identity fraud, and electronic theft.

The Indian Penal Code 1860 (IPC), which punishes offences, including those committed in cyberspace (such as defamation, cheating, criminal intimation, and obscenity), and the Companies (Management and Administration) Rules 2014 (the CAM Rules), framed under the Companies Act 2013, require companies to ensure that electronic records and security systems are secure from unauthorised access and tampering.

In addition to the previously mentioned, authorities such as the Reserve Bank of India (RBI), the Department of Telecommunication (DoT), the Insurance Regulatory and Development Authority of India Act 1999 (IRDA), and the Securities Exchange Board of India (SEBI) have issued industry specific guidelines for companies, telecom service providers, banks, insurance, and listed organizations to maintain cyber security standards.

As a comprehensive cyber security regulation, the IT Act may be viewed as an attempt to reduce cybercrime in India. The (Indian) Information Technology Act, 2000 [6] addresses issues such as compensation (Civil) and punishment (Criminal) for improper disclosure and abuse of personal data, as well as breach of contractual conditions pertaining to personal data. Sections 43, 65, 66, and 72 of the IT Act deal with data protection and data privacy.

Aside from the aforementioned legislation, the Personal Data Protection Bill was introduced in the Indian Parliament in 2019 [6]. The objective was to develop a system for preserving personal data and creating criteria for public and commercial parties to gain access. The measure establishes precise rules for personal data gathering, storage, and processing, as well as sanctions and compensation for non-compliance. The bill, however, has yet to become law. The Union government informed the Supreme Court on April 11, 2023 that a new legislation, the Digital Personal Data Protection Bill 2023 to safeguard individual privacy in online space is "ready." [8]. The new Bill was to be be tabled during the Monsoon Session of Parliament.

## V. CONCLUSION

Adopting adequate privacy and data protection policies and technology will safeguard both the individual and the organisation from unforeseen and accidental harm. As a result, becoming aware of the cyber world's flaws is essential. Several countries have recently enacted data protection and privacy legislation. However, the procedures and policies are not the same. Despite the fact that certain countries lack dedicated cyber security legislation, there are a number of laws that address data safety and security. There might be effective standards in place to protect the information we communicate in cyberspace. However, raising awareness about data theft and privacy breaches is showing positive trend. As many countries have come forward to take necessary steps to remove chances for hackers to obtain, modify and damage data.

## AUTHOR'S CONTRIBUTION

Dr. Geetha A. J. is the sole author of the present paper. She has written the article independently.

## CONFLICT OF INTEREST

The author certifies that she has no affiliation with any organisation in conducting this work or any entity with financial interest or non financial interest in the subject matter or materials discussed in the manuscript.

## FUNDING ACKNOWLEDGEMENT

The author has not received any financial support for research, authorship, and/or for the publication of the article.

## REFERENCES

[1] “What is Data Security.” IBM.com. [Online]. Available: https://www.ibm.com/topics/data-security

[2] "What is data security?" Fortinet.com. [Online]. Available: https://www.fortinet.com/resources/cyberglossary/data-security

[3] "What is data protection and privacy." Cloudian.com. [Online]. Available: https://cloudian.com/guides/data-protection/data-protection-and-privacy-7-ways-to-protect-user-data/

[4] "Data Security." Imperva.com. [Online]. Available: https://www.imperva.com/learn/data-security/data-security/

[5] S. Shea, "What is data security? The ultimate guide." TechTarget.com. [Online]. Available: https://www.techtarget.com/searchsecurity/Data-security-guide-Everything-you-need-to-know

[6] M. Manjari, "Data Protection Laws in India." iPleaders.in. [Online]. Available: https://blog.ipleaders.in/data-protection-laws-in-india-2/#:~:text=The%20Information%20Technology%20Act%2C%202000,legislation%20for%20this%20matter%20yet

[7] V. P. Dalmia, "India : Data protection laws in India - Everything you must know." Mondaq.com. [Online]. Available: https://www.mondaq.com/india/data-protection/655034/data-protection-laws-in-india---everything-you-must-know

[8] K. Rajgopal, "New digital personal data protection bill in monsoon session." The Hindu.com. [Online]. Available: https://www.thehindu.com/news/national/new-data-protection-bill-likely-to-be-introduced-in-monsoon-session-in-parliament-centre-to-supreme-court/article66723887.ece

## About the Author

**Dr. Geetha A. J.** is Assistant Professor at the department of Journalism and Mass Communication at Sri Dharmasthala Manjunatheshwara College (Autonomous) Ujire, Karnataka, Ujire. Her areas of specializations are new media, digital media literacy, media effect studies, and corporate communication.