Data integrity

Data integrity is a term used to refer to the accuracy and reliability of data. Data must be complete, with no variations or compromises from the original, to be considered reliable and accurate. Compromises to data integrity can happen in a number of ways. In industries where data is handled, identifying and addressing potential sources of damage to data is an important aspect of data security.

Problems with data integrity can start with a human source. People entering records may make mistakes, leading to variations between the original data and the data stored in a system. Likewise, people can make mistakes while transferring or copying data electronically, causing a disparity between different versions of a file or references to a file. In order for data integrity to be maintained, there need to be no changes or alterations to the data.

As data is entered, stored, accessed, moved, and updated, weak points in a system can compromise the data. Glitches in a computer may lead to partial overwrites of data or other data errors. Viruses can be created to attack data integrity, some working quietly to damage data without betraying their presence. Interruptions in various operations can lead to problems, as can mechanical damage like exposure to magnets or physical damage caused by power outages and other events.