

Data loss *



Cromino S.R.L.
Str. Florilor Nr. 148 Ap. 13
407280, Floresti, Jud
Cluj, Romania
Cell+4(075)2979579
office@secure-data.ro
www.secure-data.ro

Types of Data Loss Events

- **Intentional Action**
 - Intentional deletion of a file or program
- **Unintentional Action**
 - Accidental deletion of a file or program
 - Misplacement of CDs, DVDs, floppies or removable media
 - Administration errors
 - Inability to read unknown file format
- **Failure**
 - Power failure.
 - Hardware failure, such as a head crash in a hard disk.
 - A software crash or freeze, resulting in data not being saved.
 - Software bugs or poor usability, such as not confirming a file delete command.
 - Data corruption, such as file-system corruption or database corruption.
- **Disaster**
 - Natural disaster, earthquake, flood, tornado, etc.
 - Fire
- **Crime**
 - Theft, hacking, sabotage, etc.
 - A malicious act, such as a worm, virus, hacker or theft of physical media.



Data loss is also very common. 66% of internet users have suffered from serious data loss.

Studies have consistently shown hardware failure and human error to be two most common causes of data loss, accounting for roughly three quarters of all incidents. A commonly overlooked cause is a natural disaster. Although the probability is small, the only way to recover from data loss due to a natural disaster is to store backup data in a physically separate location.

Protect data of being lost

There is no guaranteed way to prevent data loss. However, the frequency of data loss events and their impact can be greatly mitigated by taking proper precautions. The different types of data loss events demand different types of precautions. A well rounded approach to data protection has the best chance of avoiding data loss events. User education is probably the most important, and most difficult aspect of preventing data loss. Nothing else will prevent users from making mistakes that jeopardize data security.

Backup, or making copies of data so that these additional copies may be used to restore the original is probably the best logical way to prevent data loss. Backups are useful primarily for two purposes, to:

- restore a state following a disaster
- restore small numbers of files after they have been accidentally deleted or corrupted

Since a backup system contains at least one copy of all data worth saving, the data storage requirements are considerable. Organizing this storage space and managing the backup process is a complicated undertaking. A data repository model can be used to provide structure to the storage. In the modern era of computing there are many different types of data storage devices that are useful for making backups. There are also many different ways in which these devices can be arranged to provide geographic redundancy, data security, and portability.

Before data is sent to its storage location, it is selected, extracted, and manipulated. Many different techniques have been developed to optimize the backup procedure. These include optimizations for dealing with open files and live data sources as well as compression, encryption, and de-duplication, among others.

Many organizations and individuals try to have confidence that the process is working as expected and work to define measurements and validation techniques. It is also important to recognize the limitations and human factors involved in any backup scheme.

* - In the field of information technology, data loss refers to the unforeseen loss of data or information. An occurrence of data loss can be called a Data Loss Event and there are several possible root causes. Data loss must be distinguished from data unavailability, such as may arise from a network outage. Although the two have substantially similar effects, data unavailability is temporary while data loss is permanent.