What is data destruction?

Data destruction is the deliberate deletion, corruption, or encryption of data to cause harm or cover an attacker's tracks. It shows up as ransomware, wiper malware, and insider sabotage. Unlike theft, the damage is to availability and integrity, so the only reliable defense is backups you have tested restoring, plus tightly limiting who can delete data at scale.

HOW IT WORKS

01 Where it comes from

Destruction takes a few common forms:

- Ransomware, which encrypts data and holds the key for payment.
- Wiper malware, which destroys data outright, sometimes disguised as ransomware with no working key.
- Insider sabotage, a disgruntled employee deleting or corrupting systems.
- Cloud account or key deletion, where an attacker with admin access deletes storage, snapshots, or the keys needed to decrypt.
- Accidental mass deletion, which is not an attack but causes the same outage and belongs in the same recovery plan.

02 Why it is different from theft

Stolen data is a confidentiality and compliance problem. Destroyed data is an operational one: systems stop, orders cannot be processed, and the business can halt entirely until data is restored. That is why ransomware, which weaponises availability, has been so effective.

Sophisticated attackers also destroy data to cover their tracks, wiping logs and evidence so you cannot see what they did or how they got in. That makes recovery and investigation harder at the same moment.

> ATTACKERS TARGET YOUR BACKUPS TOO
>
> *Modern ransomware hunts for and deletes backups first. A backup on the same network with the same credentials is not a backup; it is a second target. Offline or immutable copies are what actually survive.*

HOW TO DEFEND

- Keep 3-2-1 backups (three copies, two media types, one off-site) and, crucially, make at least one immutable or offline so an attacker with admin cannot delete it.
- Test restores. A backup you have never restored is a guess.
- Limit who can delete at scale. Least privilege and multi-factor authentication on cloud and backup admin accounts.
- Turn on versioning and soft-delete where your platforms offer it.
- Monitor for mass-deletion and encryption so you catch it early.

SOURCES

[1] Data Destruction (Technique T1485)

[2] StopRansomware

[3] Computer Security Resource Center Glossary

Find out whether an attacker could reach and delete your backups.

securelayer7.net/learn/threats/data-destruction

Open online