The Shared Responsibility Model and the Importance of Cloud Backup

47% of data loss is caused by end user deletions.

This is called the **Shared Responsibility Model.**

The Shared Responsibility Model was created by Microsoft to outline who is responsible for data in different scenarios of data loss. SaaS vendors are only responsible for data protection and data loss **some** of the time. That means end users are responsible for data security and data loss the **rest** of the time.

Responsibility	SaaS	PaaS	IaaS	On-prem	
Information and data	●	●	●	●	
Devices (Mobile and PCs)	●	●	●	●	**Responsibility always retained by customer**
Accounts and identities	●	●	●	●	
Identity and directory infrastructure	◐	●	●	●	
Applications	○	◐	●	●	**Responsibility varies by service type**
Network controls	○	○	●	●	
Operating system	○	○	◐	●	
Physical hosts	○	○	○	●	
Physical network	○	○	○	●	**Responsibility transfers to cloud provider**
Physical datatcenter	○	○	○	●	

● Microsoft ● Customer

SaaS - Software as a Service
PaaS - Platform as a Servive

IaaS - Infrastrcuture as a Service
On-prem - On premises

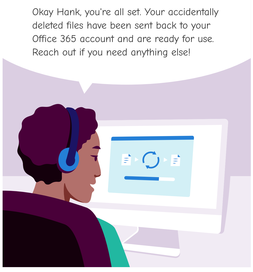
Microsoft states for all cloud deployment types (SaaS, PaaS, IaaS):

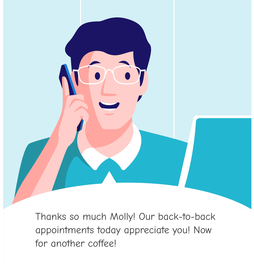
"You are responsible for protecting the security of your data and identities.

Regardless of the type of deployment, the following responsibilities are

always retained by you: Data, Endpoints, Account, Access management."

- Microsoft on data loss caused by imminent disruptions and outages





Backup your backups

Just because your data is in the cloud, it doesn't mean you can't lose it. While SaaS applications offer many advantages, they can't completely protect your business data from human error or ransomware attacks .

According to a study by The Aberdeen Group on data loss in the cloud:

47% were due to end-users deleting information

17% were users overwriting data

13% were because hackers deleted info

With Datto's SaaS Protection and our expert help, you can avoid downtime and keep business data more secure. **Get in touch today to learn more about our backup offerings.**