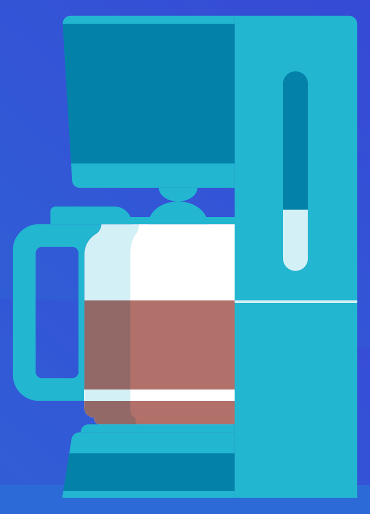
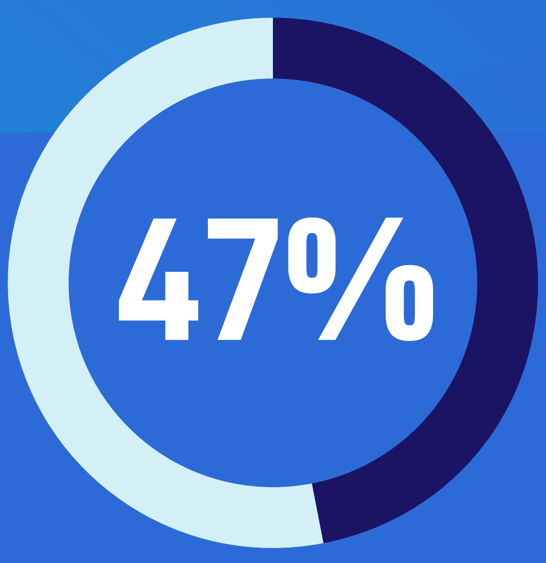
The Shared Responsibility Model and the Importance of Cloud Backup



Did You Know?



of data loss is caused by end-user deletions.

What is 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	●	●	●	●	Responsibility always retained by customer
Devices (Mobile and PCs)	●	●	●	●	
Accounts and Identities	●	●	●	●	
Identity and Directory Infrastructure	◐	◐	●	●	Responsibility varies by service type
Applications	○	◐	●	●	
Network Controls	○	◐	●	●	
Operating System	○	○	●	●	
Physical Hosts	○	○	○	●	Responsibility transfers to cloud provider
Physical Network	○	○	○	●	
Physical Datatcenter	○	○	○	●	

○ Microsoft ● Customer

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

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

> “We strive to keep the Services up and running; however, all online services suffer occasional disruptions and outages, and Microsoft is not liable for any disruption or loss you may suffer as a result. In the event of an outage, you may not be able to retrieve Your Content or Data that you’ve stored. We recommend that you regularly backup Your Content and Data that you store on the Services or store using Third-Party Apps and Services.”

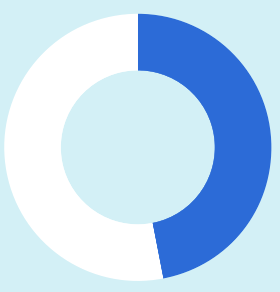
- Microsoft on data loss caused by imminent disruptions and outages

With iCorps 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.**

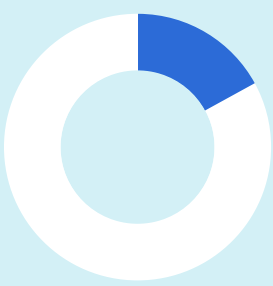
Backup Your Backups

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 .

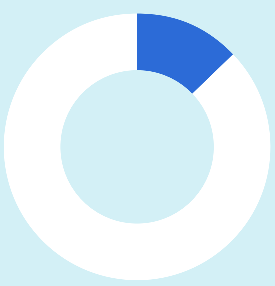
According to a study by The Aberdeen Group on data loss in the cloud:



47% were due to end-users deleting information



17% were users overwriting data



13% were because hackers deleted info

iCorps TECHNOLOGIES