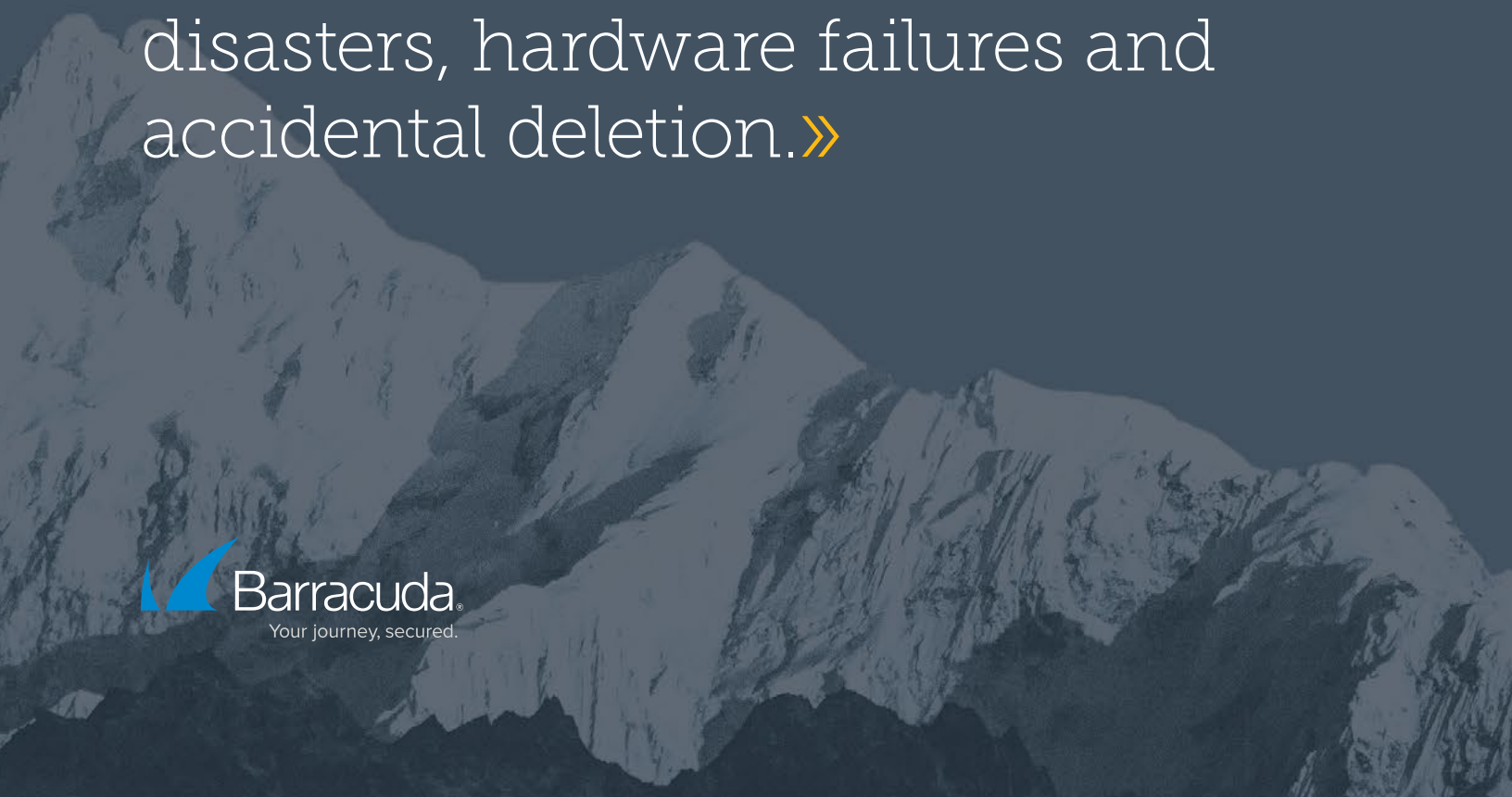
Market Analysis: Closing Backup and Recovery Gaps

Limit Your Organization's Exposure to IT Risk

IT professionals have evolving attitudes and approaches about backing up and recovering data to deal with ransomware, natural disasters, hardware failures and accidental deletion.»



Barracuda
Your journey, secured.

Table of Contents

Strategies shift with evolving threats

Backup and recovery are essential for the modern IT professional, and not just because of the threat of ransomware, natural disasters and hardware failures. These incidents might grab the headlines, but the more mundane prospect of employees accidentally deleting key emails and documents is a far more prevalent threat to most organizations.

Data is the lifeblood of every modern business, driving billions of dollars in digital innovation and growth every year. Every organization needs to ensure data is accurate and up-to-date. Every organization must also be able to recover data in a timely manner after an outage, mistake or serious cyber-attack.

As such, backup is a key component of any best-practice approach to IT risk management. Most organizations would be at a standstill without access to email and data.

Data is the lifeblood of every modern business...»

Global perspectives on backup

Barracuda dug a little deeper, to understand how IT professionals around the world are handling this key IT competence:

- What kind of data and systems are being included in backup plans
- How cloud backup is growing in popularity – and what may be holding it back
- Why confusion about backing up Office 365 data is increasing organizational risk

See the full survey results for yourself: This report includes all the latest findings, including what every organization should look for when it comes to a backup and recovery solution.

Why confusion about backing up Office 365 data is increasing organizational risk.»

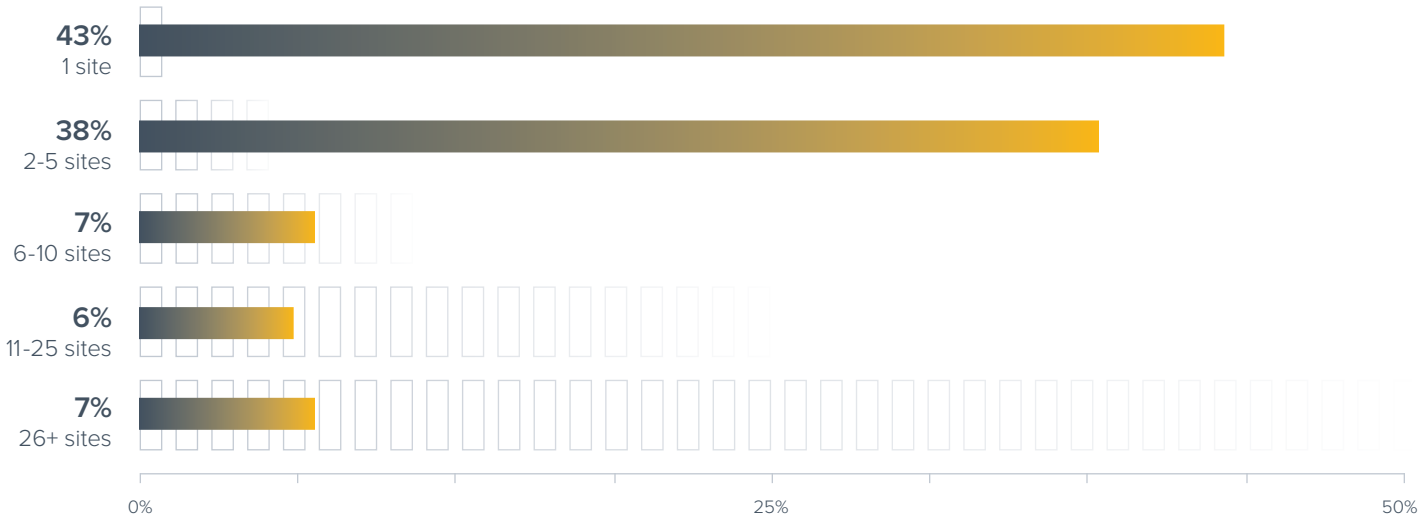
Methodology

Barracuda surveyed more than **1,000 IT professionals**, business executives and backup administrators to find out more about their data-protection strategies.

Respondents represent a broad cross section of sectors and organizations, ranging in size from less than **50 employees to more than 5,000**. Organizations in all global regions were included in the survey.

Backup demands are growing

How many sites do you backup? N=1,091



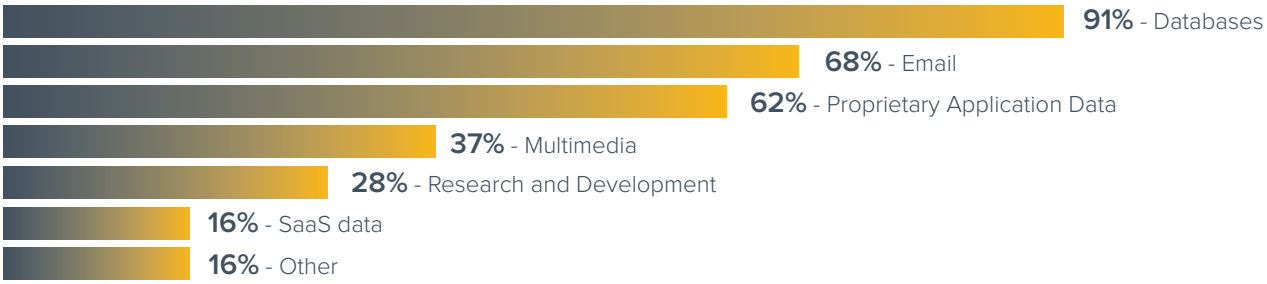
The modern IT administrator faces a major challenge. The majority of respondents to our study are tasked with managing backups from multiple sites. In some cases **(7%), they must do so for more than 26 sites**, although **more than half (57%) back up more than two sites**. Either way, this makes remote management a key consideration for any backup and recovery solution, to help save valuable IT time and effort during day-to-day tasks and urgent recovery efforts.

When you combine this data with the new push for multi-cloud deployments, it's clear the simpler days of companies managing a single site and on-premises architecture are a thing of the past.

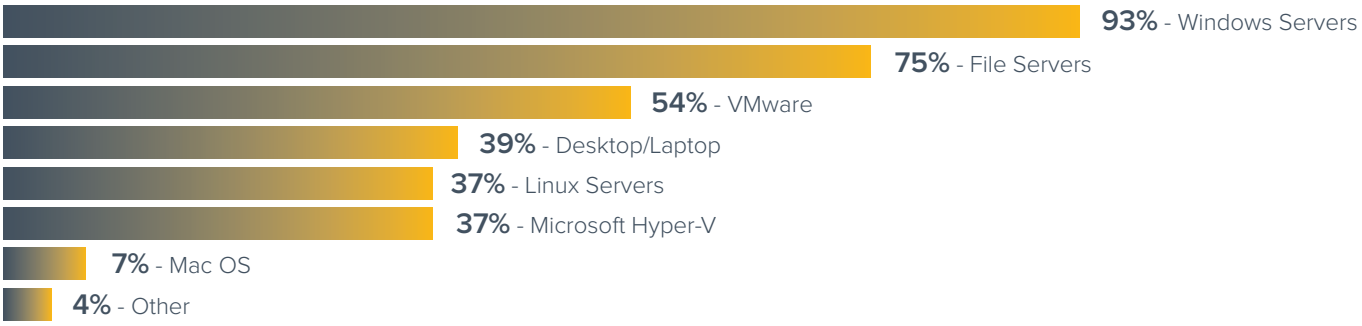
Key Findings

- 7% of IT administrators back up more than 26 sites
- 57% of IT administrators back up more than two sites

What types of data do you protect? N=1,090



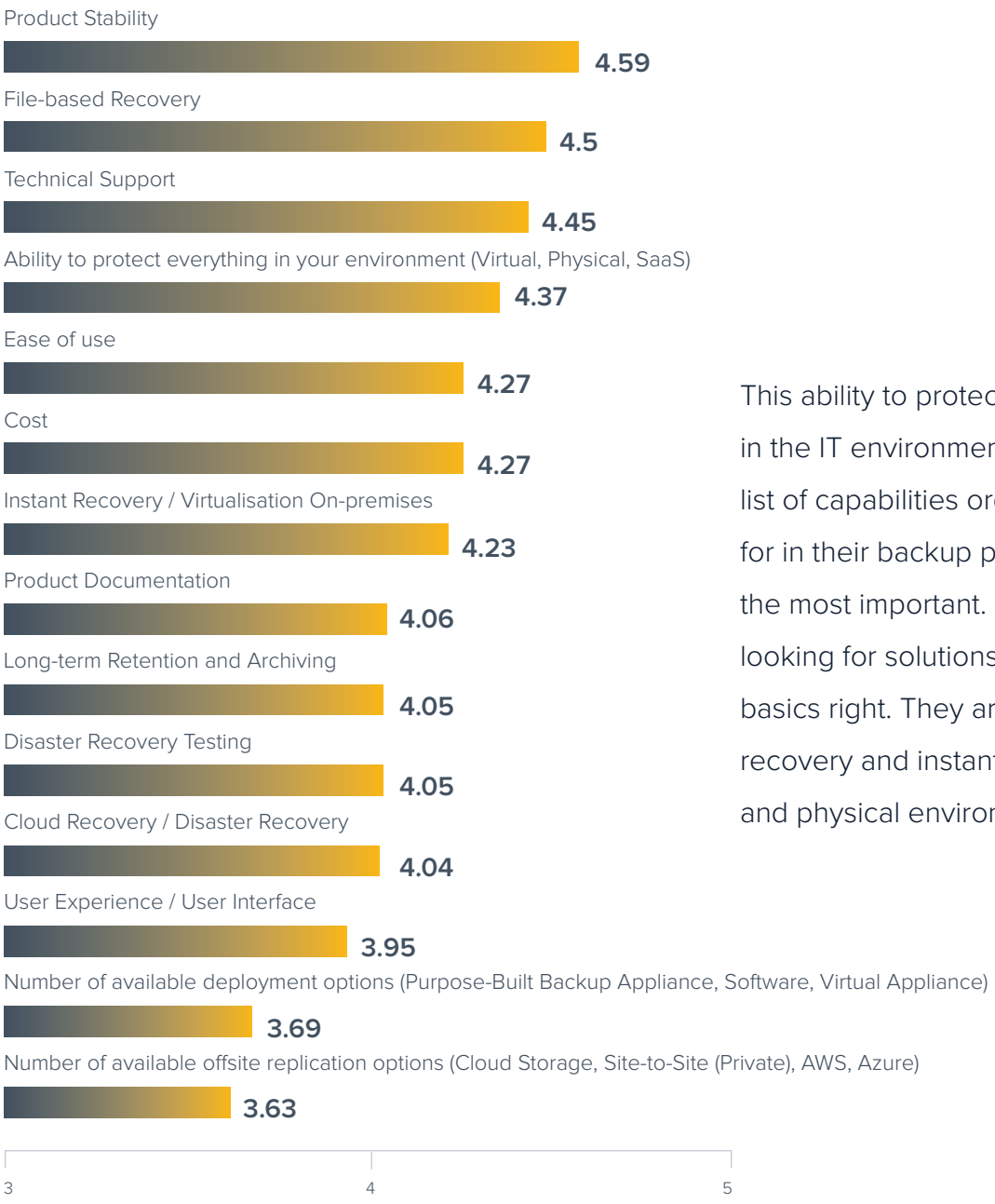
What types of servers and storage devices do you protect? N=1,085



Increasingly, everything is deemed mission critical today. Email, database, application, R&D, and even multimedia data was cited by large numbers of respondents as protected by backups. Linux, Windows, Mac OS, Hyper-V, desktop/laptop, file servers, VMware environments and more were also name-checked. This highlights the importance of choosing a backup provider that can support a wide variety of data types and physical/virtual/cloud systems.

However, of some concern is the small number of respondents **(16%) wanting to back up their SaaS data**. This inaction is putting their business continuity at risk.

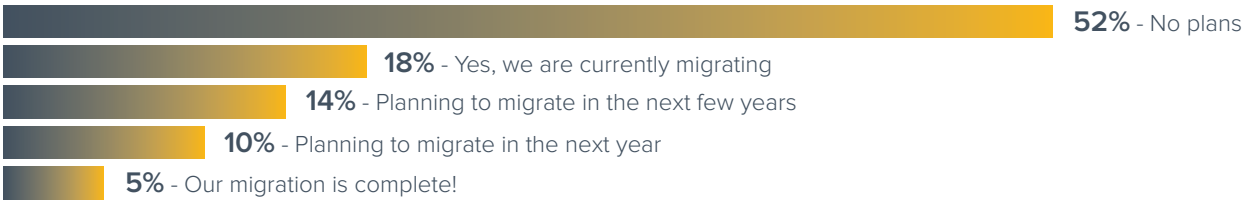
On a scale of 1-5, with 1 being not at all important to you and 5 being very important to you, please rate the following areas of a backup solution: N=1,082



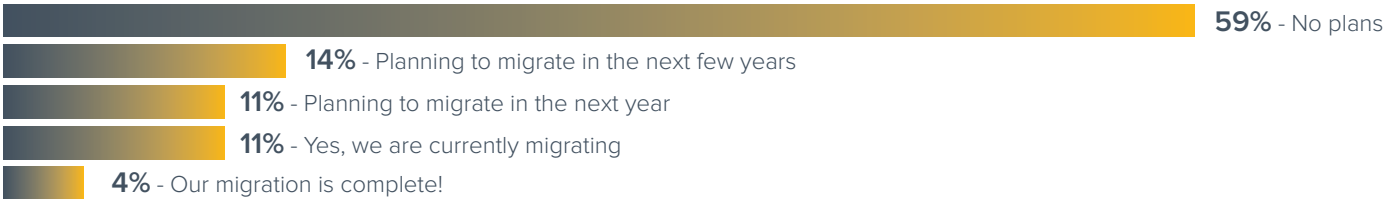
This ability to protect data across all systems in the IT environment was just one of a long list of capabilities organizations are looking for in their backup provider, albeit one of the most important. In many ways, firms are looking for solutions that simply get the basics right. They are also keen on file-based recovery and instant recovery across virtual and physical environments.

Global cloud migration varies by service

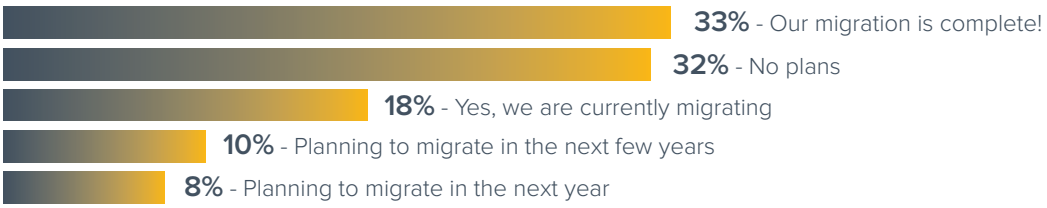
Are you migrating applications to the public cloud? N=1,030



Are you migrating file services to the public cloud? N=1,019



Are you migrating email services to the public cloud? N=1,018



Organizations appear to be somewhat hesitant about migrating data to the cloud. **A majority claim they have no plans to migrate apps (52%) or file services (59%)** to these environments in the future. That's not the case with email, however, with 33% having already migrated and 34% more currently doing so or planning to soon.

For those that do migrate, cloud backup can be a great way to manage risk across these environments. It can offer a more affordable, effective, reliable and easier-to-manage option than many on-premises solutions.

A third of firms still don't back up to the cloud

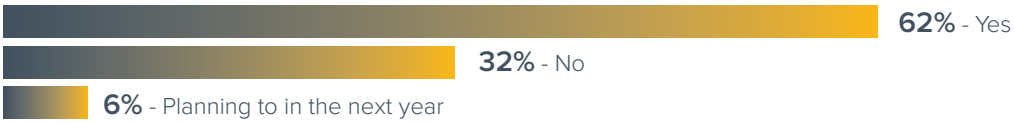
Do you replicate your backup data to the cloud? N=1,088

Although the majority **(64%) of global organizations said they back up data to the cloud in this way**, **a sizeable minority (36%) still doesn't**. It's unclear why this is, although there could be latent security concerns over doing so.

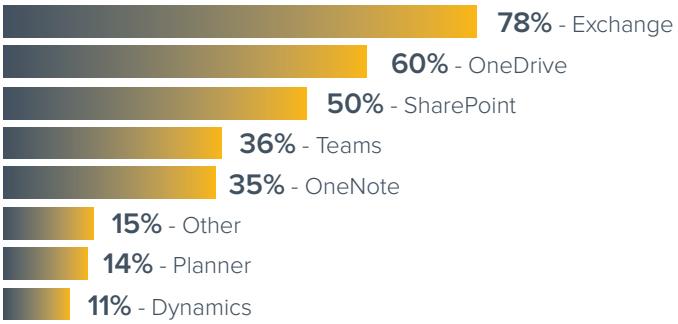
Organizations could be exposing themselves to greater risk by not using cloud backup as one of their options. If they're simply replicating to alternative sites, those facilities could all be taken out by the same natural disaster, especially if located in the same region. Industry best practice is to back up according to the 3-2-1 rule: at least three copies, in two different formats, with one copy stored offline or in the cloud. This is an important consideration, especially for those in highly-regulated industries.

Office 365 confusion is exposing firms to significant risk

Do you currently use Office 365? N=1,012

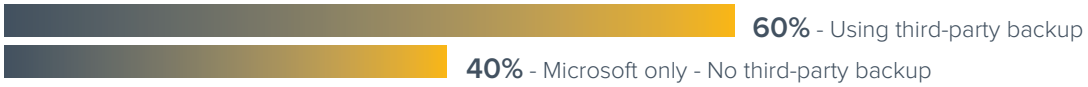


If yes, which Office 365 applications does your organization currently use? N=791



Office 365 is one of the most popular cloud-based productivity platforms. **More than 60% of IT professionals** are using it to drive business success. **Email is most popular (78%)**, although firms are also making increased use of a range of other apps in the platform, **including SharePoint (50%), OneDrive (60%), Teams (36%) and OneNote (35%).**

Are you using third-party software to backup Office 365? N=766



There is a major challenge: a sizeable minority **(40%) aren't using any third-party backup tools to protect mission-critical data** because they believe that Microsoft provides all the backup they need. This is unlikely to be true. While Microsoft provides a resilient SaaS infrastructure to ensure availability, it does not protect data for historical restoration for long and its SLAs don't protect against user error, malicious intent or other data-destroying activity.

In fact, deleted emails are not backed up in the traditional sense; they are kept in the Recycle Bin for a maximum of 93 days before they're deleted forever. On SharePoint and OneDrive, deleted information is retained for a maximum of 14 days by Microsoft and individuals must open a support ticket to retrieve it. SharePoint and OneDrive are unable to retrieve single items/files; they must restore an entire instance. It's unlikely that such short retention policies will meet most compliance requirements.

Choosing the right backup and recovery solution

Global organizations understand the importance of backup and recovery for the modern, risk-focused IT function. They want to protect a wide range of data and systems — including on-premises, virtual and cloud environments — across multiple sites, ideally via the same solution. Yet there are concerning gaps in their awareness. A sizeable minority still hasn't embraced cloud backup solutions, despite the undoubted benefits. Plus, there are gaps in awareness about the need for backing up SaaS data, which could be putting companies at risk.

Many incorrectly assume that Microsoft will support their backup requirements for Office 365 data. This could be a costly mistake. If they suffer a serious incident, they could find that crucial data has been deleted permanently.

The good news is that there are plenty of advanced third-party backup and recovery solutions offering exactly what these organizations are demanding: protection via a single product and user-friendly interface across all data types and sources; superb technical support; file-based recovery and more. IT managers keen to support business growth and keep the regulators happy should revisit their backup strategies to ensure there are no gaps in coverage.

Choose a backup and recovery solution that protects data no matter the source. When you can replicate to the public cloud, private cloud or another physical device, you can protect everything and recover quickly in the face of accidental deletion, malicious actions or a disaster.