# Data Protection in the Age of the Cloud

# White Paper

# Introduction

Barracuda recently conducted a comprehensive survey of 200 customer organisations in Europe, the Middle East, and Africa (EMEA). The goal of the survey was to gain a clear understanding of how customers are addressing the need for backup in the age of distributed, cloud-integrated networks.

The majority of organisations that participated in our survey have to protect multiple locations, typically with both virtual and physical machines running different operating systems, including other systems such as storage devices. In many cases, modern infrastructures are hybrid. Some systems are deployed locally and some are cloud-based, using various IaaS and SaaS offerings. All of those systems and all of the data stored on those systems need to be protected against loss, whether that is caused by malware, natural disaster, or human error.

Many organisations employ a combination of different backup solutions for different parts of their network, or for different classes of data. However, such fragmented strategies can make it hard to restore lost files in a disaster-recovery scenario within a reasonable timeframe. The goal of a modern data protection strategy should be to enable fast, complete data recovery that minimises downtime following a loss of critical data.

Cloud-integrated backup solutions make it possible to rapidly provision infrastructure, in principle allowing for faster and easier return to normal operations. Nevertheless, many survey participants did not report using the cloud for either primary backup or offsite replication.

The survey's core finding, therefore, is that there is still a large gap between the capabilities and potential for cloud-integrated backup and its actual adoption by Barracuda customers in EMEA. As IT and security decision-makers become more aware of how much cost, effort, and downtime can be avoided with the adoption of a modern, cloud-replicated data protection solution, we expect to see an acceleration in the adoption of such solutions among organisations of all sizes in EMEA, as organisations have done in other parts of the world.

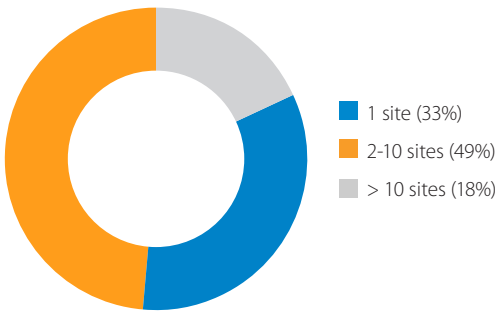
# Methodology

Barracuda Networks conducted the survey in September 2017 with 200 customer organisations in Europe, the Middle East, and Africa. That ranged from very small (0-1 employees) to very large (>10,000 employees), in a wide range of industries.

# Distributed and hybrid environments

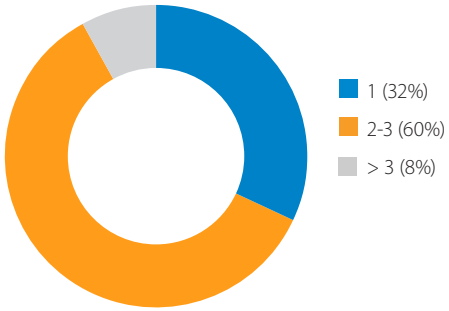
The majority of survey respondents report that they are protecting more than one location, with two-thirds needed to protect more than one location, and about 18 percent have to protect more than 10 sites.

**How many sites do you backup?**



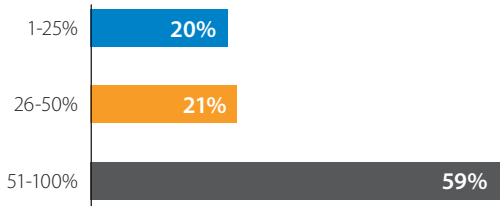

Those environments are being protected using multiple backup products. Responses have shown that only 32 percent of organisations can meet their data protection requirements using only one backup solution. 61 percent use two or three different solutions, while 7 percent of the respondents need more than three different products to protect their data.

**How many different backup products do you use?**

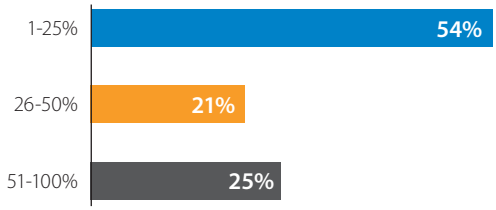



Responses clearly show that tape backups are widely considered obsolete. 59 percent of respondents are protecting more than half of the data using modern disk-based backups, and 54 percent responded that less than one quarter of their data is backed up on tapes.

**What percentage of your backups are disk-based?**



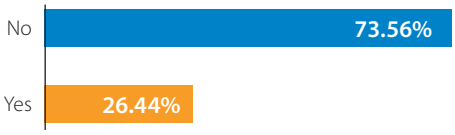

**What percentage of your backups are tape-based?**



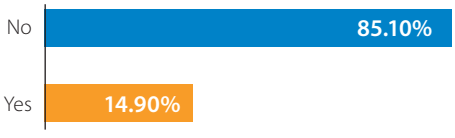

Protecting hybrid intrastructures such as physical and virtual servers in distributed environments can be challenging, but it can also enable sophisticated replication scenarios between sites. Organisations with only one location do not have the option of easily establishing reduntant replication across sites.

Replication to public cloud environments is an option to ignore site-to-site bandwidth limitations and to avoid single-point failures in central locations such as headquarters. Cloud-integrated backup solutions can also reduce up-front costs and complexity of traditional backup products. Nevertheless, the majority of respondents are not currently replicating data to the cloud. The amount of cloud-based backups is small as well, with 75 percent reporting that less than one quarter of their backups are cloud-based.

**Do you replicate your data to the Cloud?**



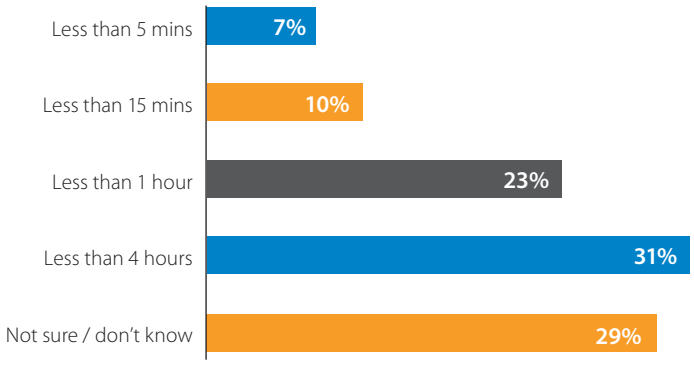

**Do you currently backup to Public Cloud?**



## Ambitious goals

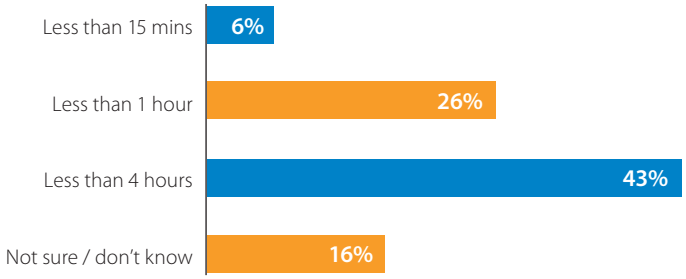
Despite the fragmented data protection strategies using different backup products across multiple locations, requirements regarding recovery point objective and recovery time objective are high. Among the 70 percent of respondents who knew about the requirements in their organisation, 31 percent are backing up the most important applications and data at least every four hours, 21 percent cannot afford to lose more than one hour's worth of work and changes, and 17 percent create backups every 15 minutes or more frequently. Almost 30 percent are not sure or do not know about RPO requirements.

**What is your RPO goal for your most important applications/data?**




Respondents had broadly similar responses when asked about recovery time objectives. Whereas 16 percent do not know or are not sure, the majority of 43 percent considers anything less than four hours to be an acceptable restoration time. About one quarter require systems to be back up and running in less than one hour, and 6 percent have a recovery time objective of less than 15 minutes.

**What is your RTO goal for your most important applications/data?**

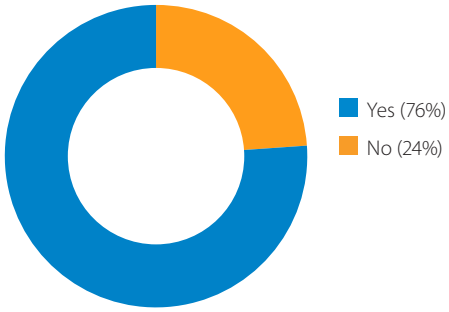



It's clear that many organisations are aware of the challenges and difficulties involved in meeting short recovery time goals. About half of our respondents say they are fairly confident in their ability to meet these goals, but 20 percent are not confident at all, and only 25 percent are sure they can meet their goals in a disaster situation.

## Disaster recovery

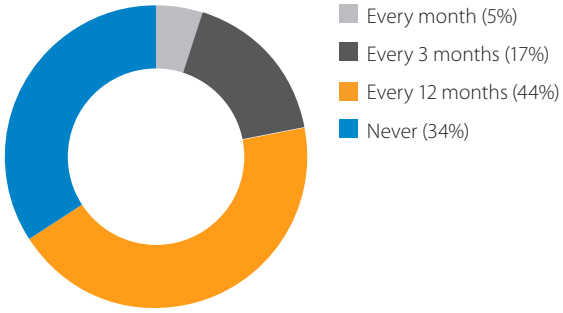
Asking organisations about disaster recovery plans and testing confirmed the assumption that can be made looking at RPO and RTO targets. Organisations are aware of the risks, but are so far having difficulty mitigating them. One-fourth of respondants report that they do not have a disaster recovery plan in place.

**Do you have a Disaster Recovery plan?**



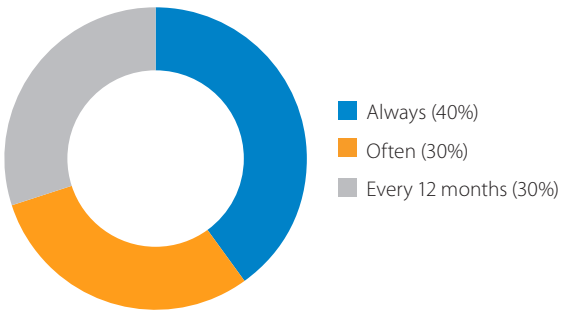

Having a disaster recovery plan is important, but if it is not tested, it is likely to fail in an emergency. 65 percent validate their disaster recovery plan regularly, at least once a year. 34 percent do not test disaster recoveries at all, and because 24 percent of the participants do not have plan in place, we can assume that 10 percent of organisations with a disaster recovery plan do not validate it. All those organisations are at risk.

**How frequently do you test your Disaster Recovery (DR) plan?**



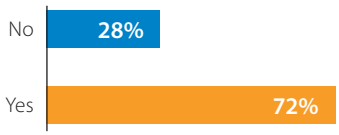

A disaster recovery plan that is tested but does not successfully complete its test is a clear motivator to making improvements to the backup strategy. Only 40 percent of survey respondents report that they have a disaster recovery plan that always completes testing successfully. 30 percent answered that their plan often works as intended.

**How often does your DR test complete successfully?**




The importance of disaster recovery is confirmed by the finding that 72 percent of respondents have already had to restore an entire system or application.

**Have you ever had to restore an entire system or business application?**



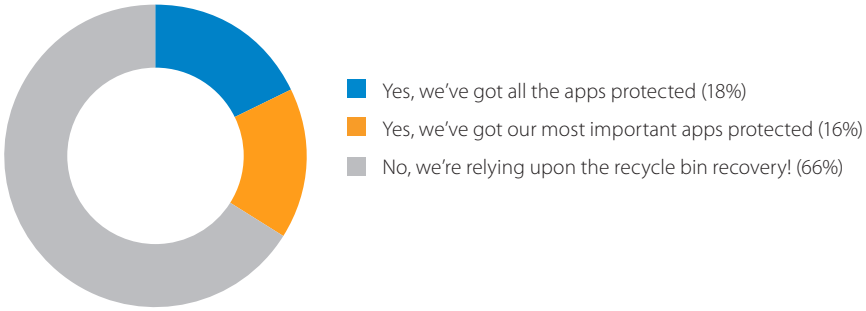
**Have you ever had a backup fail to restore?**


More ominously, over half of respondents have experienced a failure to resore backup files. Considering that restoring backup is usually the last option when all attempts to repair failed, it is likely that those cases resulted in data loss.

## Backing up SaaS applications

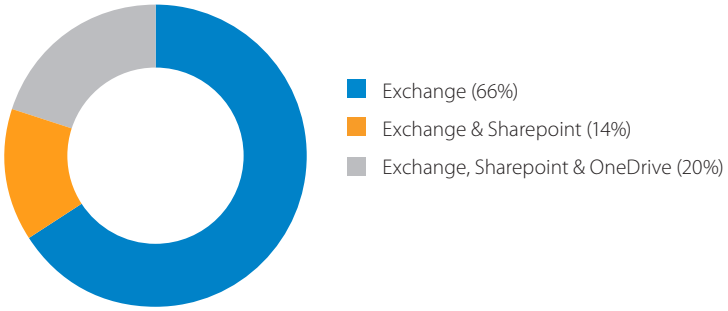
As opposed to on-premises environments, where most organisations are somewhat prepared for disasters, respondents using Microsoft Office 365 were found to be considerably less prepared for data losses or disasters. 66 percent of respondents rely completely on the built-in recycle bin for recovery. Only 18 percent have all their apps and data protected, with 16 percent protecting at least the most important applications and data.

**Are you backing up your Office 365 data?**




Out of those who do back up their Office 365 data, 66 percent protect Exchange data only, but not the remaining applications. Only 20 percent are backing up Exchange, SharePoint, and OneDrive data.

**Does your Office 365 backup product/service protect Exchange, Sharepoint & OneDrive?**




Without backup protection, data in Office 365 is at risk. Cloud services should not be considered a replacement for data protection solutions. Vendors typically offer limited native restore capabilities, and refer to third-party solutions for customisable solutions.

## Conclusion

Changing environments require new approaches to disaster recovery. Organisations are well aware that on-premises infrastructure needs to be covered, and that effective, regularly tested disaster recovery plans need to be in place. Our respondents tended to have fairly ambitious goals regarding recovery time, but they are generally not confident they can meet these goals.

With a significant majority of respondents reporting that they use more than one backup solution, there is a significant opportunity for our respondents to reduce costs, complexity, and recovery times through consolidation.

Although the percentage of tape-based backups still in use is small compared to other technologies, those still have a negative impact on respondents' restore requirements, as restoration typically is complicated and/or requires manual interaction.

The widespread adoption of advanced, cloud-connected solutions such as Barracuda Backup—which uses features such as LiveBoot to enable very rapid server restores, and extends encrypted, redundant backup capabilities across hybrid architectures—would enable many organisations to improve their ability to meet ambitious recovery time objectives while reducing administrative overhead and simplifying backup management.

In addition, for users of Office 365 and other SaaS applications delivered via cloud, the use of a comprehensive security and data-protection solution such as Barracuda Essentials could simplify regulatory and e-discovery compliance while also helping to meet time-to-recovery objectives.

Disaster recovery is about much more than advanced threats and ransomware. It is equally about getting back up and running following a simple human error, a hardware failure, or a natural disaster. Regardless of the cause, the ability to recover quickly from disaster is critical to protecting reputations and brands, and to preventing the potential costs of extended downtime.

## About Barracuda Networks, Inc.

Barracuda simplifies IT with cloud-enabled solutions that empower customers to protect their networks, applications, and data regardless of where they reside. These powerful, easy-to-use, and affordable solutions are trusted by more than 150,000 organizations worldwide, and are delivered in appliance, virtual appliance, cloud, and hybrid configurations. Barracuda's customer-centric business model focuses on delivering high-value, subscription-based IT solutions that provide end-to-end network security and data protection. For additional information, please visit barracuda.com.



Barracuda

Barracuda Networks Inc
Brunel House, Stephenson Road, Houndmills, Basingstoke, RG21 6XR, United Kingdom

**t:** +44 (0) 1256 300 100
**e:** emeainfo@barracuda.com
**w:** barracuda.com