


THE VALUE OF CLOUD DATA PROTECTION FOR REMOTE OFFICE / BRANCH OFFICE

July 2019

Derek E. Brink, CISSP

Vice President and Research Fellow, Information Security and IT GRC



In previous research, Aberdeen quantified how the *faster, more scalable time-to-recover enterprise data* provided by a **cloud-based backup and restore** capability *reduces the business impact of unplanned downtime by about 90%* compared to traditional, on-premises approaches. In this report, Aberdeen extends its analysis to show how these benefits are amplified when applied to **remote office / branch office (ROBO)** scenarios.

Context: What Do ROBO Scenarios Look Like?

In **remote office / branch office (ROBO)** scenarios the enterprise consists of *multiple sites*, each of which has its own number of employees and their associated data.

From a data protection perspective, virtually all ROBO sites need data backup and restore capabilities for enterprise **endpoints** — and larger ROBO sites also need data backup and restore capabilities for enterprise **server rooms / data centers**.

To provide context for this report, Aberdeen did an analysis based on its extensive visibility into current installations of data protection technologies. Across *more than 10,000 sites at more than 2,000 enterprises* in *14 industry sectors*, this yielded the following insights:

- ▶ **The number of unique sites per enterprise** (remote offices / branch offices) ranges from 1-35, with a median of three
- ▶ **The number of employees per site** ranges from 1-2,000, with a median of 25

ROBO scenarios can be especially challenging for the organization's IT staff. *All data* must be backed up, available, and swiftly recoverable — but remote and branch offices commonly lack the people, processes, and technologies necessary for timely and cost-effective data backup and recovery.

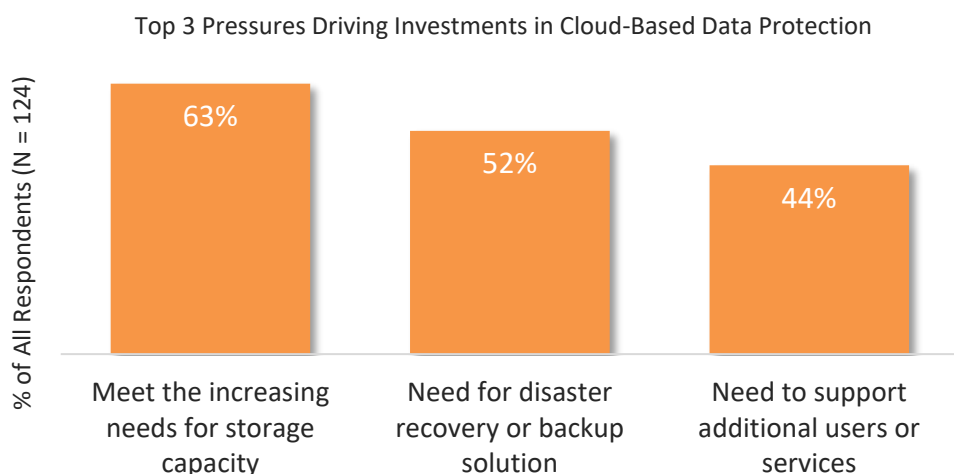
Organizations see **a move to cloud-based data protection strategies** as a *flexible, consistent, and cost-effective* way to address their relentless

In **remote office / branch office (ROBO)** scenarios, the enterprise consists of multiple sites — each of which has its own number of employees and their associated data that must be backed up, available, and swiftly recoverable.

requirements for *growth*, while also addressing their increasing *risks*. For example, respondents to Aberdeen's traditional benchmark research identified the following as the **top three pressures driving their investments in cloud-based data protection solutions** (Figure 1):

- ▶ **Increasing need for data storage capacity** (63%)
- ▶ **Increasing need for a data backup and restore / disaster recovery solution** (52%)
- ▶ **Increasing need to support additional enterprise users and services** (44%) — without corresponding growth in IT staff

Figure 1: To Help Address Growth and Risk, Organizations Look to Data Protection in the Cloud



Source: Multiple responses accepted, does not add to 100%; Aberdeen, July 2019

Recap: Quantifying the Value of Data Protection in the Cloud

In its previous research report, *Reducing the Impact of Ransomware Attacks with Cloud-Based Backup and Restore*, Aberdeen's analysis quantified ransomware risk for **traditional enterprise endpoints** using current, on-premises approaches to data backup and restore:

- ▶ For an organization of 1,000 users and 10 TB of data that potentially needs to be recovered, the **median** annual business impact of ransomware is **about \$480K**, with a **10% likelihood** of being **more than \$2.5M**.

From a data protection perspective, virtually all ROBO sites need data backup and restore capabilities for enterprise **endpoints** — and larger ROBO sites also need data backup and restore capabilities for enterprise **server rooms / data centers**.

After deployment of a **cloud-based backup and restore** solution:

- ▶ The **median** annual business impact of ransomware in this scenario is reduced to **about \$54K** (including the incremental cost of the solution), with a **10% likelihood** of being **more than \$200K**.
- ▶ The *faster, more scalable time-to-recover* provided by deploying a cloud-based backup and restore solution helps to reduce the risk of ransomware for enterprise endpoints by **more than 90%**.

The reason is simple: Faster, more scalable time-to-recover enterprise data from a wide range of sources, which increasingly includes **mobile devices, connected devices (IoT), on-premises servers, and cloud-based services** in addition to traditional **enterprise endpoints** significantly reduces the total cost of lost productivity for enterprise users. It should go without saying, but *all* enterprise data should be backed up, available, and recoverable, regardless of the source.

In Aberdeen's analysis — which assumed a single enterprise site with 1,000 employees and a total 10 TB of traditional endpoint data potentially in need of recovery — the total time-to-recover was based on empirical performance data made available by a specific solution provider (*Druva*).

Extending the Analysis: Remote Office / Branch Office (ROBO)

Using these insights, along with the same estimates for the amount of traditional endpoint data that potentially needs to be recovered (10 TB for every 1,000 employees) and total time-to-recover, Aberdeen has extended its analysis to quantify the value of using a cloud-based backup and restore solution — as compared to the use of traditional, on-premises approaches — in ROBO scenarios:

- ▶ **Using traditional, on-premises approaches to data protection** — the **median** total cost of lost user productivity from data backup and restore is **about \$2.5M per year**, with a **10% likelihood of exceeding \$20M**.
- ▶ **Using a cloud-based backup and restore solution**, the **median** total cost of lost user productivity from data backup and restore is reduced to **about \$75K per year** (including the incremental cost), with a **10% likelihood of exceeding \$500K**.

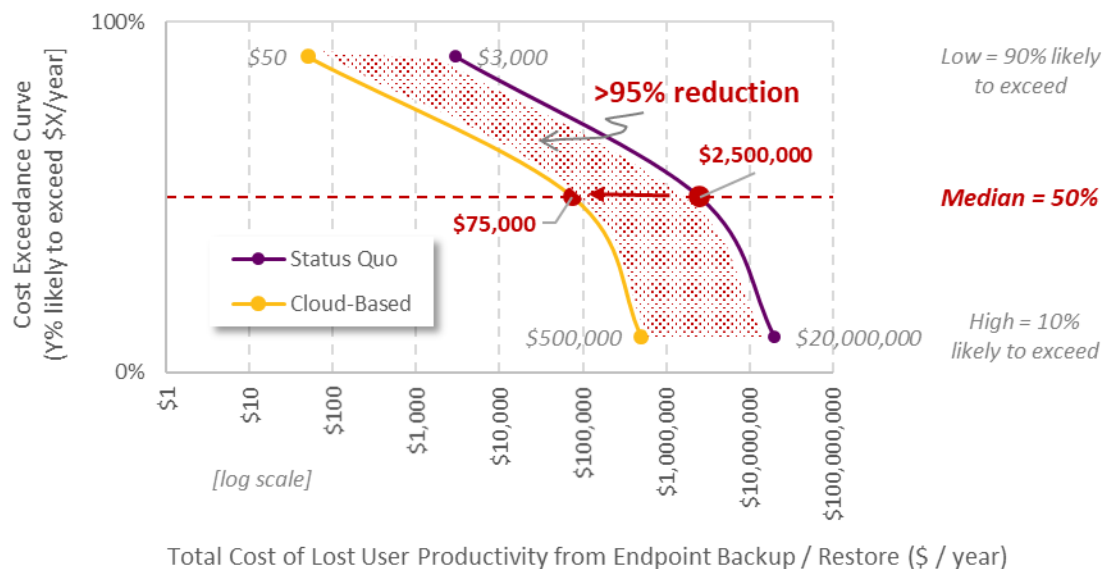
In other words: Aberdeen's analysis shows that the faster, more scalable time-to-recover provided by using a cloud-based backup and restore solution helps to reduce the total cost of lost productivity for enterprise

To help the organization's senior leadership team **make better-informed business decisions about the risks** of data protection — and what to do about them — security professionals need to communicate these issues more effectively, in the language of risk that senior leaders already know and understand: *how likely*, and *how much business impact*?

Aberdeen's analysis shows that the use of a cloud-based backup and restore solution reduces the total cost of lost productivity for enterprise users in ROBO scenarios by **more than 95%**, as compared to the use of traditional on-premises approaches.

users in remote office / branch office scenarios by **more than 95%** as compared to the use of traditional, on-premises approaches (Figure 2).

Figure 2: Cloud-based Backup and Restore Results in >95% Reduction in Total Cost for Remote Office / Branch Office Scenarios



Source: Monte Carlo analysis, Aberdeen, July 2019

Given the above, it's no surprise that **enterprise buyers are shifting to cloud-based backup and recovery solutions** over traditional, on-premises approaches to data protection.

Summary and Key Takeaways

Aberdeen's analysis helps to illustrate how **by moving data protection to the cloud**, enterprises can:

- ▶ **Significantly reduce the total business impact** of data backup and restore activities
- ▶ **Recapture lost productivity of users** and technical staff for the pursuit of strategic business objectives
- ▶ **Dramatically improve speed and consistency of protecting data** — a benefit which is amplified when applied to remote office / branch office (ROBO) scenarios



Related Research

- ▶ *Reducing the Impact of Ransomware Attacks with Cloud-Based Backup and Restore*; March 2019
- ▶ *Quantifying How Disaster Recovery in the Cloud Reduces Your Risk: It's About Time*; December 2018
- ▶ *Quantifying How Disaster Recovery as a Service Reduces Your Risk from Disruptions*; August 2018
- ▶ *Enterprise Data in 2018: The State of Privacy and Security Compliance*; March 2018

About Aberdeen

Since 1988, Aberdeen has published research that helps businesses worldwide to improve their performance. Our analysts derive fact-based, vendor-neutral insights from a proprietary analytical framework, which identifies Best-in-Class organizations from primary research conducted with industry practitioners. The resulting research content is used by hundreds of thousands of business professionals to drive smarter decision-making and improve business strategies. Aberdeen is headquartered in Waltham, Massachusetts, USA.

This document is the result of primary research performed by Aberdeen and represents the best analysis available at the time of publication. Unless otherwise noted, the entire contents of this publication are copyrighted by Aberdeen and may not be reproduced, distributed, archived, or transmitted in any form or by any means without prior written consent by Aberdeen.