QUANTIFYING HOW DISASTER RECOVERY IN THE CLOUD REDUCES YOUR RISK: IT’S ABOUT TIME
Fast, reliable time-to-recover is a key factor in reducing the business impact of a disruption to the availability of your business-critical applications and data. Aberdeen’s analysis quantifies the business value of restoring your data and getting your applications back up and running more quickly, and shows how the core value propositions for Disaster Recovery in the Cloud solutions are well-aligned with enterprise needs.

An Empirical Enterprise Hierarchy of Needs: First Data Storage, Then Data Backup / Restore, Then Disaster Recovery

Aberdeen’s large-scale analysis of enterprise online research activities highlights an empirical enterprise hierarchy of needs: first data storage, then data backup and restore, then disaster recovery (see Figure 1).

Figure 1: Enterprise Interest in Data Storage, Data Backup and Restore, and Disaster Recovery Reflects a Hierarchy of Needs

The implied hierarchy of needs seen in Aberdeen’s analysis shows that enterprises place their priorities first on operational necessity (data storage), then on operational contingency and best practice (data backup and restore), and finally on proactive reduction of risk from operational disruptions (disaster recovery).

For every enterprise actively researching the topic of data storage, about 4 out of 5 (81%) are also researching data backup and restore, and nearly 3 out of 5 (57%) are researching disaster recovery. On reflection, the implied hierarchy of needs seen in this analysis is unsurprising — it shows that enterprises place their priorities first on operational necessity, then on operational contingency and best practice, and finally on proactive reduction of risk from operational disruptions.
Every organization needs data storage. In the context of protecting that data and reducing the risk of non-availability, it’s also easy to appreciate that data backup and restore and disaster recovery are essential activities — but what actually delivers business value is the successful and timely recovery and resumption of operations after a disruption. Ultimately, investments in capabilities for data backup and restore and disaster recovery are a risk-based business decision, as opposed to solely a tactical technology decision.

Faced with an unplanned disruption to the availability of the organization’s business-critical applications and data, the most basic operational questions for IT and security staff to address for the senior leaders are:

- Is our data backed up?
- How quickly can our data be recovered and restored?
- How quickly can our critical applications be back up and running?

In Aberdeen’s view, the key to increasing the ratios seen in Figure 1 closer to 100% across the board is quantifying the business value — properly, in terms of both how likely and how much business impact — of fast, reliable time-to-recover.

Said another way, the fundamental business value of data backup and restore and disaster recovery is about reducing the organization’s risk of non-availability to an acceptable level. That is, such risks can never be completely eliminated, only managed to within the organization’s appetite for risk — where risk is described properly in terms of both:

- How likely a disruption to business-critical applications and data is to happen, in a given period of time, and
- How much business impact it could have if a disruption to business-critical applications and data does in fact occur.

**Breaking Down the Risk of Disruptions: How Likely?**

The likelihood of disruptions to the availability of your business-critical applications and data is undeniably real. For example, Aberdeen’s benchmark research provides empirical insights into the frequency and duration of unplanned downtime events, based on the responses of more than 120 diverse organizations (see Figure 2):
Over the previous 12 months, the likelihood of experiencing unplanned downtime of business-critical applications was 92%.

The median duration of disruptions to business-critical applications over the last 12 months was about four hours, but had a “long tail” of more than four days.

Figure 2: Empirical Non-Availability of Business-Critical Applications and Data (Annual Minutes of Disruption)

A median of four hours means that half of the time, the annual duration of non-availability was less than this, i.e., in the realm of two 9s (99.99%), three 9s (99.999%), and below. But it also means that half of the time, the annual duration of non-availability was more than four hours, up to and including a non-trivial likelihood of lasting more than four days. This is the potentially catastrophic long tail of risk that is so commonly seen in IT operations and cyber security — and which is so important for technical staff to help senior business leaders understand, to help them make a better-informed business decision about it.

Breaking Down the Risk of Disruptions: How Much Impact?

The business impact of disruptions to the availability of your critical applications and data can be significant. It can also be quantified — or at least estimated within a reasonable range, given the inherent uncertainties in these measurements. Keep in mind that the goal is to help senior business leaders move the dial for decision making away from mere intuition, judgment calls, and gut feel — which is about the best they can do based on the information they are usually provided with:

Source: Aberdeen, December 2018
► Technical details about what can potentially go wrong, and how;

► Headlines about what other companies have already experienced, based on public disclosures;

► Qualitative assessments of risk based on “red, yellow, and green” or “high, medium, and low,” and pseudo-quantitative derivate which misguided translate colors into numbers;

► Misleading and falsely precise “statistics” based on single-point estimates, such as “the average cost of a data breach is $201 per record.”

For example, four high-level categories of the potential business impact from unplanned disruptions to business-critical applications and data are summarized in Table 1.

**Table 1: High-Level Categories of the Potential Business Impact from Non-Availability of Business-Critical Applications and Data**

<table>
<thead>
<tr>
<th>Potential Business Impact</th>
<th>Factors for Quantification of Business Impact (Illustrative)</th>
</tr>
</thead>
</table>
| Lost productivity of users during the time of disruption                                  | ▪ Number of users
▪ Fully loaded cost of user time
▪ Percentage of user productivity lost during the time of disruption (i.e., as opposed to merely redirected) |
| Loss of current revenue during the time of disruption                                     | ▪ Revenue generated from critical applications and data
▪ Percentage of revenue lost during the time of disruption (i.e., as opposed to merely delayed or deferred) |
| Cost of response and recovery from disruption                                             | ▪ Number of responders
▪ Fully-loaded cost of responder time
▪ Total cost of tools for response and recovery                                           |
| Loss of future profitability (lower revenue, higher costs) as a result of disruption       | ▪ Customer defection to competitors
▪ Customer non-renewal of subscription relationships
▪ Higher costs to retain existing customers, attract new customers
▪ Other observable effects of damage to reputation / brand                                 |

Source: Aberdeen, December 2018
An Example of Quantification: How a One-Hour SLA for a Disaster Recovery in the Cloud Solution Reduces the Business Impact of a Disruption

As an example of quantifying the risk of non-availability — and the business value of investing in a Disaster Recovery in the Cloud solution with a contractually committed time to get business-critical applications back up and running — Aberdeen has developed a simple Monte Carlo analysis based on the following assumptions:

- **Current state (status quo):** The factors of likelihood, recovery times, and business impact are modeled based on the empirical data seen in Aberdeen’s benchmark research.

- **Future state (reduction in business impact from a one-hour SLA from a Disaster Recovery in the Cloud solution):** All else being equal, the uncertainty of time-to-recover is reduced to one hour — effectively cutting off the “long tail” of non-availability risk.

To be useful for a specific enterprise, this kind of analysis requires personalization based on the nature of the applications and data, the amount of revenue they generate, and the number of users they support — i.e., the organization-specific values for the factors enumerated in Table 1. For the purposes of this example, Aberdeen’s analysis is based on $200M in annual revenue and 1,000 business users. Compared to the status quo approach to disaster recovery:

- **For every $200M in annual revenue,** a one-hour time-to-recover reduces the annualized business impact of unplanned disruptions by a **median of about $60K**, and cuts off the “long tail” of risk by **more than $2.6M**.

- **For every 1,000 users,** a one-hour time-to-recover reduces the annualized business impact of unplanned disruptions by a **median of about $40K**, and cuts off the “long tail” of risk by **more than $2.0M**.

Why Wouldn’t Every Enterprise Invest in Disaster Recovery Capabilities to Ensure Faster Time-to-Recover — And Should They Invest in “Build” (On-Premises) or “Buy” (Cloud)?

Based on these results, why wouldn’t *every* enterprise invest in disaster recovery capabilities that ensure the delivery of a one-hour SLA? Aberdeen’s benchmark research provides some insight into this question,
in that the top three *inhibitors* for investments in disaster recovery capabilities are lack of *internal expertise to plan* (selected by 38% of all respondents; multiple responses accepted), lack of *internal staff to implement* (38%), and lack of *budget* (35%).

In other words, organizations say they don’t invest in faster and more consistent disaster recovery capabilities because they lack the in-house *expertise, time, and budget* — all three of which are well-aligned with the core value propositions for a *Disaster Recovery in the Cloud solution, which*:

- **Addresses the risk of disruption** to critical applications and data
  - As opposed to ignoring or accepting the risk (i.e., no disaster recovery capability at all), including the potentially catastrophic “long tail”
  - Provides higher assurance of quickly and reliably getting critical applications back up and running
  - Supports the best practice of geographically separating primary and secondary sites (e.g., in the case of a regionalized natural disaster)

- **Captures the strategic and operational advantages** of “buy” vs. “build” for an important activity
  - Leverages the focus, expertise, and infrastructure of specialized cloud service providers
  - Allows the organization’s internal resources to stay focused on its strategic reasons for existence (e.g., serving customers, producing goods and services, and so on)
  - Aligns budgetary issues with business value (i.e., ongoing operating expense (OpEx), as compared to up-front capital expense (CapEx))
  - Provides automatic access to ongoing technical advancements and operational maturity from the cloud service provider (e.g., continuous replication, service-level agreements, validation and testing, and so on)

Historically, Aberdeen’s benchmark research has shown that disaster recovery capabilities have been in the vanguard of moving from the datacenter to the public cloud, confirming the alignment of Disaster Recovery in the Cloud solutions with the enterprise hierarchy of needs.
datacenter to the public cloud, confirming the alignment of Disaster Recovery in the Cloud solutions with the enterprise hierarchy of needs.

Of course, what action the senior business leaders in any given organization will ultimately decide to take as a result of this analysis is by no means certain. That is, they may decide to accept the current risk (e.g., by staying with the status quo of no disaster recovery capability); transfer the risk to another party (e.g., by buying an appropriate level of cyber insurance); or take steps to manage the risk to an acceptable level (e.g., by investing in a Disaster Recovery in the Cloud solution). As always, the role of the IT and security professional is to advise and recommend — it falls to the senior business leaders to decide, based on the organization’s appetite for risk.

Summary and Key Takeaways

► Enterprises exhibit an empirical hierarchy of needs: first data storage, then data backup and restore, then disaster recovery.

  o In Aberdeen’s view, the key to increasing the maturity of enterprise backup / restore and disaster recovery capabilities is quantifying the business value — properly, in terms of both how likely and how much business impact — of fast, reliable time-to-recover.

  o Ultimately, investments in these kinds of capabilities are a risk-based business decision, as opposed to solely a tactical technology decision.

► Fast, reliable time-to-recover is a key factor in reducing the business impact of an unplanned disruption to the availability of your business-critical applications and data.

  o Aberdeen’s analysis quantifies the value of a one-hour time-to-recover — such as might be provided by a Disaster Recovery in the Cloud solution — for restoring your data, and getting your applications back up and running:

    ▪ Lower loss of revenue between $0 – $2.6M per year (median of about $60K) for every $200M.

    ▪ Lower loss of user productivity between $0 – $2M per year (median of about $40K) for every 1,000 users.
Aberdeen’s research shows that organizations don’t invest in faster and more consistent disaster recover capabilities because they lack the in-house expertise, time, and budget — needs which are well-aligned with the core value propositions for a Disaster Recovery in the Cloud solution, which:

- **Addresses the risk of disruption** to critical applications and data, as opposed to ignoring or accepting the risk, including the potentially catastrophic “long tail,” and

- **Captures the strategic and operational advantages** of “buy” vs. “build” for an important activity, by leveraging the focus, expertise, and infrastructure of specialized cloud service providers.
About Aberdeen Group

Since 1988, Aberdeen Group 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 Group is headquartered in Waltham, Massachusetts, USA.

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