RR

HOW DISASTER RECOVERY IN THE CLOUD REDUCES YOUR RISK: IT'S ABOUT TIME

July 2020

Derek E. Brink, CISSP
Vice President and Research Fellow, Information Security and IT GRC

ABERDEEN

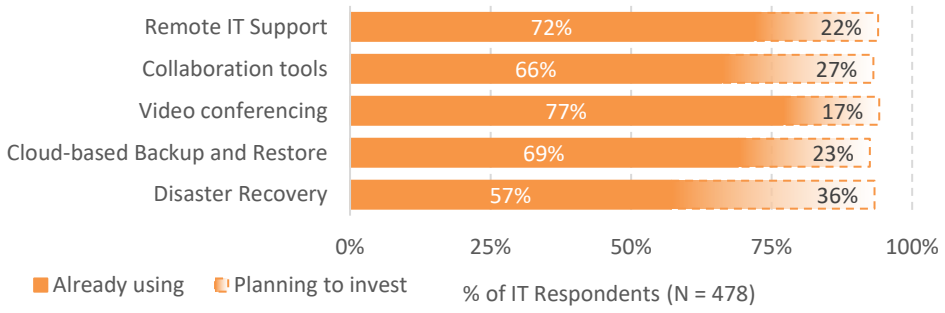
Fast, reliable time-to-recover is a key factor in reducing the business impact of an unplanned disruption to the availability of your business-critical applications and data. Aberdeen's analysis quantifies the business value of restoring your data and getting your applications back up and running more quickly, and shows how the core value propositions for **Disaster Recovery in the Cloud** solutions are well-aligned with enterprise needs — particularly in an expanded WFH era.

The Evolving Enterprise Hierarchy of Needs: First Data Storage, Then Data Backup / Restore, Then Disaster Recovery

Traditionally, Aberdeen's large-scale analysis of enterprise online research activities has highlighted an empirical enterprise *hierarchy of needs*: first **data storage**, then **data backup and restore**, then **disaster recovery**. More recently — given the abrupt and widespread changes in where and how the organization's work gets done, as a result of the pandemic of 2020 — Aberdeen's research has shown how these priorities have changed.

In a dramatically expanded Work From Home (WFH) / Work From Anywhere (WFA) environment, it's not surprising that enterprises are giving priority to the things that are most important: *Get their users up, running, and productive* — and *keep them up, running, and productive*.

Figure 1: Top Five IT / Data Management Technologies Deployed to Cope with Post-Pandemic IT Operations



Source: 2020 *Aberdeen Business Review*; Aberdeen, July 2020

The implied hierarchy of needs seen in Aberdeen's research has traditionally shown that enterprises have placed 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**). These priorities have been updated in the wake of the pandemic of 2020.

It goes without saying: Every organization needs data storage, and a lot of it. For the respondents in Aberdeen's study, the total volume of active business data is large (median: more than 250 terabytes) and growing rapidly (median: more than 20% per year).

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*. As seen in Figure 1, both of these technologies were among the top five identified by respondents as essential to cope with post-pandemic IT operations.

But to be clear: The value these activities actually deliver to the business is the successful and timely **recovery** and **resumption of operations** after an unplanned disruption. 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?

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. In other words, the fundamental business value of data backup and restore and disaster recovery is about reducing the organization's **risk** of non-availability — properly described, in terms of both *how likely* and *how much business impact* — 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** an unplanned 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.

For IT and security staff communicating with senior business leaders about data backup and restore and disaster recovery, it's essential to distinguish between our technical activities (*what we do*, *how we do it*) and the resulting business value those activities create (*why it matters*).

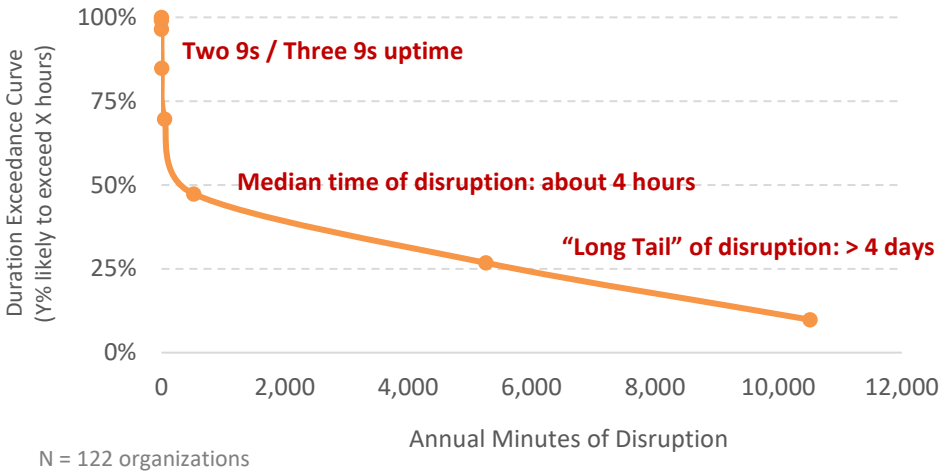
Breaking Down the Risk of Disruptions: How Likely?

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 (see Figure 2):

- **Frequency:** In the *2020 Aberdeen Business Review*, nearly all (**94%**) respondents experienced at least one unplanned downtime event per month — a number consistent with previous research.
- **Duration:** Over the last 12 months, the **median** duration of unplanned disruptions to business-critical applications at more than 120 diverse organizations was reported as **about four hours** — but the **"long tail"** duration of these disruptions was **more than four days**.

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



N = 122 organizations

Source: Aberdeen, July 2020

To help senior leaders make a better-informed business decision about the risk of disruption to business-critical applications and data, technical staff needs to communicate the *range of possible occurrences* — not a falsely precise *single-point estimate*.

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% uptime)*, *three 9s (99.999% uptime)*, 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 regarding what to do about it.

Breaking Down the Risk of Disruptions: How Much Impact?

The *business impact* of unplanned 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, gut feel, and judgment calls — which is about the best they can do based on the information they are usually provided with, i.e.,:

- *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* derivates which misguidedly translate colors into numbers
- *Misleading and falsely precise "statistics"* based on single-point estimates, such as "the average cost of a data breach is $148 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

Potential Business Impact	Factors for Quantification of Business Impact (illustrative)
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 to other activities)
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 to a later time)

Cost of response and recovery from disruption	▪ Number of responders ▪ Fully-loaded cost of responder time ▪ Total cost of tools and services 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, July 2020

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 normalized for *$200M in annual revenue* and *1,000 enterprise 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**.

SLA: Service Level Agreement

Disaster Recovery in the Cloud: a disaster recovery solution from a managed service provider or a cloud service provider, as opposed to a traditional, on-premises implementation

- **For every 1,000 enterprise 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)

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.

- 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.

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)
- 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 simply to **advise** and **recommend**. It falls to the senior business leaders to **decide**, based on the organization's **appetite for risk** — a topic which the pandemic of 2020 has sharply shifted from a mere abstraction to a concrete imperative.

Summary and Key Takeaways

- Traditionally, enterprises have exhibited an empirical *hierarchy of needs*: first **data storage**, then **data backup and restore**, then **disaster recovery**. More recently — given the abrupt and widespread changes in where and how the organization's work gets done, as a result of the pandemic of 2020 — data backup and restore and disaster recovery were among the top five IT / Data Management technologies identified by respondents as essential for coping with post-pandemic IT operations.

- **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.
    - 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: about $60K) for every $200M.
        - **Lower loss of user productivity** between $0 – $2M per year (median: about $40K) for every 1,000 enterprise 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.
- 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.

Related Research

Modern Backup and Recovery: Identifying the Key Drivers for Secure Enterprise Cloud Backup; May 2020

Quantifying How Disaster Recovery in the Cloud Reduces Your Risk; December 2018

Cloud-Based Backup and Virtualization: Beginning the Move to Hybrid Cloud; December 2018

The Accidental Chief Data Officer: How IT Staff Can Deliver on the Needs of Business Users; August 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.

18165