KB

HOW FASTER DATABASE RECOVERY REDUCES YOUR RISK

November 2017

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

ABERDEEN

Aberdeen's analysis shows that an *engineered systems* approach to data protection — as exemplified by the Oracle Zero Data Loss Recovery Appliance — **increases the rate of recovery** from unplanned disruptions to business-critical applications and data **by 1.5 times to 3.3 times,** as compared to traditional incremental backups, with a **median of 2.5 times**.

Business Context: Backup is Activity, Recovery is Value

In the context of database protection, **backup** is clearly an essential activity — but successful and timely **recovery** is what actually delivers the business value. Faced with an unplanned disruption to the availability of critical applications and data, the most basic operational questions to address for senior business leaders are:

- Is our data backed up?
- Is our data recoverable — do we have good data to restore?
- How quickly can our data be restored and recovered?

Speed of recovery is a key factor in reducing the risk of disruption to critical applications and data, and as such is the primary focus of this Knowledge Brief.

Fundamentally, the business value of data protection is about reducing the organization's **risk** of non-availability to an acceptable level. As always, risk is properly defined in terms of both **how likely** a disruption to critical applications and data is to happen, as well as **how much business impact** it could have if a disruption does in fact occur.

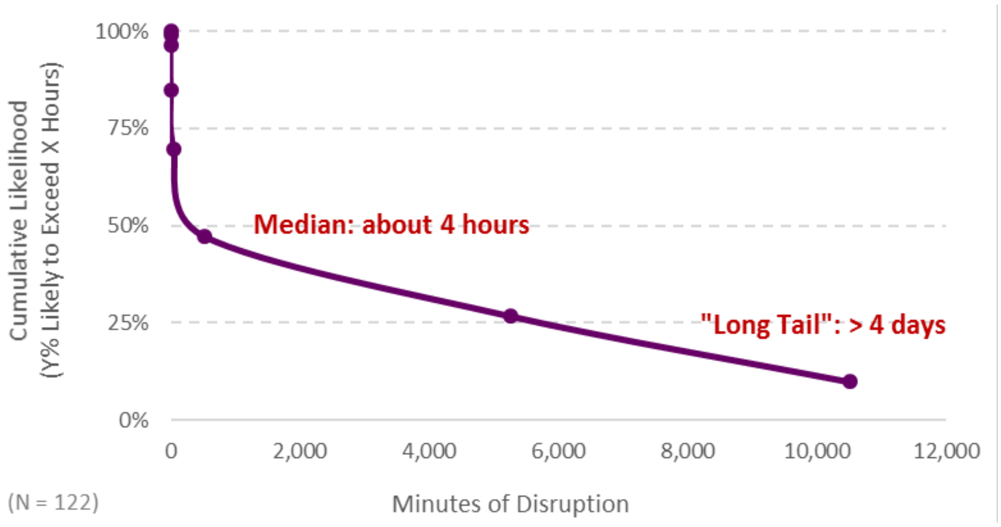
Read the Full Report: **It's About Time: How Faster Database Recovery Reduces Risk**

Breaking Down the Risk of Disruptions to Your Critical Applications and Data

The *likelihood* of disruptions to the availability of critical applications and data is very real. Aberdeen's benchmark research provides insights into the frequency and duration of unplanned downtime events, based on the responses of more than 120 diverse organizations:

- The likelihood of experiencing unplanned downtime of critical business applications over the last 12 months was **92%**.
- The **median** duration of disruptions to critical business applications over the last 12 months was **about 4 hours**, but had a “long tail” of **more than 4 days** (see Figure 1).

Figure 1: Empirical Non-Availability of Critical Applications and Data



Source: Aberdeen Group, November 2017

The *business impact* of disruptions to the availability of critical applications and data can also be significant. Some high-level categories of the potential business impact from unplanned disruptions to critical applications and data are enumerated in Table 1.

Table 1: Potential Business Impact from Unplanned Disruptions to Critical Applications and Data (Illustrative)

Business Impact	Factors
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)
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 revenue (or higher future costs) as a result of disruption	For example: ▪ Customer defection to competitors ▪ Customer non-renewal of subscriptions ▪ Higher costs to retain existing customers

Source: Aberdeen Group, November 2017

Different Technical Approaches to Protecting Critical Infrastructure Yield Different Results

Aberdeen's extensive visibility into current technology installations provides strong, market-based evidence for two contrasting technical approaches for maximizing the value of IT infrastructure:

- **A bottom-up, infrastructure-centric approach**, as exemplified by the Cisco / EMC / VMware / VCE vision for *converged infrastructure*. To the extent that buyers view their investments in computing infrastructure primarily as **technology** initiatives, the bottom-up, converged infrastructure approach will continue to gain significant traction.
- **A top-down, application-centric approach**, as represented by the Oracle vision for *engineered systems*. To the extent that buyers view their investments in computing infrastructure primarily as **application** initiatives, the top-down, engineered systems approach will have the greatest strategic appeal.

In Aberdeen's view, organizations should place the greatest strategic focus on those things which are closest to their strategic business objectives. In other words, enterprise strategies should be driven most strongly by their business-critical applications and data, rather than by their supporting IT infrastructure.

For example, Table 2 reflects Aberdeen's analysis of 1,022 enterprises, 40 solution providers and 336 associated technologies, and 66,456 technology installations. All of the installations in this snapshot were verified within the previous three years, and all had visibility into at least five out of six layers of a simple six-layer technology stack.

- **Business-critical applications and data**
- **Management / orchestration layer**
- **Virtualization layer** (e.g., hypervisors)
- **Servers** (e.g., x86, RISC)
- **Storage** (e.g., SAN, NAS)
- **Networking** (e.g., routers, switches, hubs)

Table 2: Aberdeen's Visibility into Current Technology Installations Highlights Contrasting Technical Approaches for Maximizing Value

		Selected Solution Providers						
Six-Layer Technology Stack		**Oracle**	Microsoft	IBM	**Cisco**	**Dell / EMC**	NetApp	HPE
6	Business-critical applications / data	**12,495**	8,345	5,426				
5	Management / orchestration layer		2,325	99			18	72
4	Virtualization layer (e.g., hypervisors)	**207**	986					
3	Servers (e.g., x86, RISC)	**292**		564	**546**	**203**		1,177
2	Storage (e.g., SAN, NAS)	**210**	550	672		**3,440**	2,666	1,015
1	Networking (e.g., routers, switches, hubs)				**8,243**	**66**		58
	Total Installations	**13,204**	12,206	6,761	**8,789**	**3,709**	2,684	2,322
		Top-down, application-centric approach			**Bottom-up, infrastructure-centric approach**			

Source: Aberdeen Group, November 2017

In Aberdeen's view, organizations should place the greatest strategic focus on those things which are closest to their strategic business objectives. In other words, enterprise strategies should be driven most strongly by their business-critical applications and data, rather than by their supporting IT infrastructure. For this reason, Aberdeen expects that even more enterprises will adopt the engineered systems approach for their critical applications and databases.

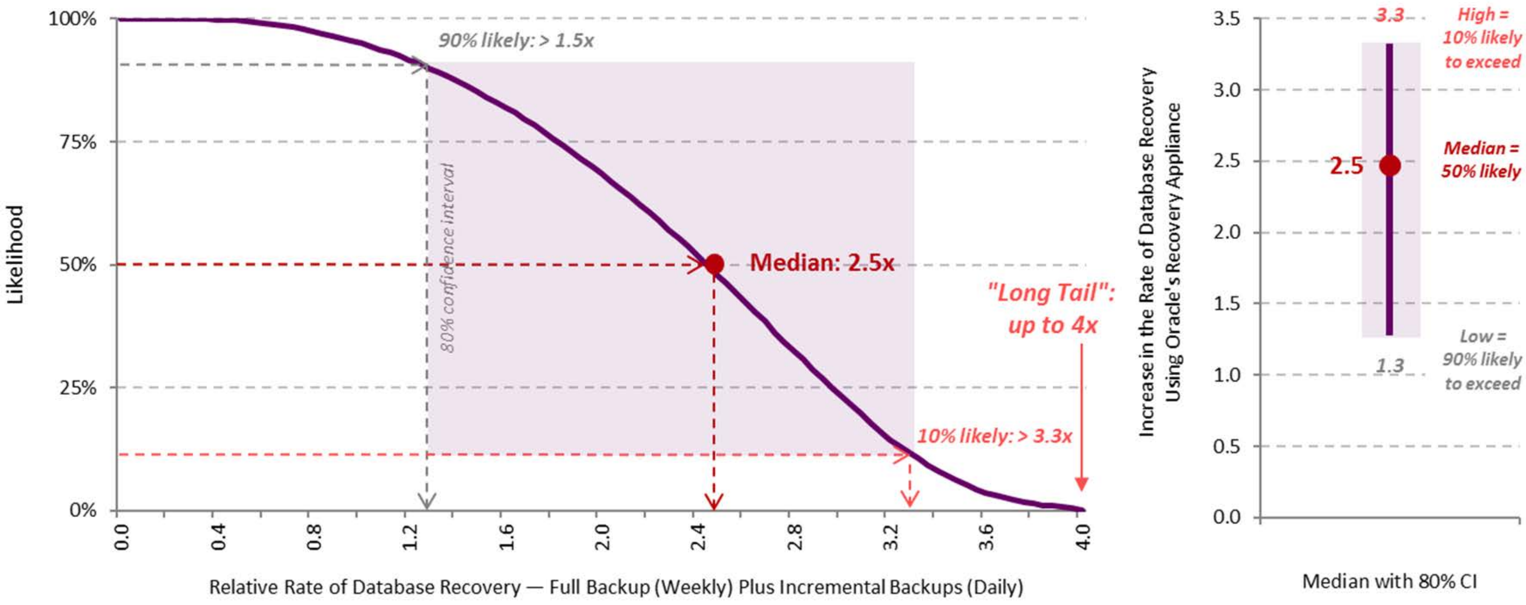
Case-in-Point: How an Engineered Systems Approach to Database Protection Increases the Rate of Recovery

To illustrate how an engineered systems approach to database protection can significantly increase the rate of recovery — and thereby reduce the risk of disruption to critical applications and data — Aberdeen has developed a simple *Monte Carlo* analysis, based on the following assumptions:

- The status quo is based on the traditional approach of **full database backups done weekly**, **and incremental database backups done daily**.
- Daily backups range **between 2% and 4%** of the total data volume.
- The number of days from the last full backup when the need for recovery occurs varies **between 0 and 6**. In the best case, recovery is based on restoring the full weekly backup. In the worst case, recovery is based on restoring the full weekly backup, plus serially restoring and applying six daily incremental backups.
- Based on its purpose-built design, the **Oracle Zero Data Loss Recovery Appliance** has *two performance advantages* that are incorporated into Aberdeen's modeling estimates. First, knowledge of file structures and data locations allow optimization that takes advantage of high-bandwidth sequential I/O capabilities, as compared to the random I/O characteristics of the status quo. Second, dynamic construction of a "virtual full backup" on the appliance eliminates additional time to serially restore and apply incremental daily backups, as is required under the status quo.

Based on these estimates, Aberdeen's analysis shows that an engineered systems approach to data protection — as exemplified by the *Oracle Zero Data Loss Recovery Appliance* — **increase the rate of recovery** from unplanned disruptions to business-critical applications and data **by 1.5 times to 3.3 times** as compared to traditional incremental backups, with a **median of 2.5 times**. See Figure 2.

Figure 2: An Engineered Systems Approach to Database Protection Increases the Rate of Database Recovery by a Median of 2.5 Times



Source: Monte Carlo analysis; Aberdeen Group, November 2017

To fully translate *faster time to recover* into a *reduction in risk* requires revisiting the examples of potential business impact from unplanned disruptions to critical applications and data that were outlined in Table 1. This is a straightforward analysis, but to be useful for a given enterprise it requires personalization based on the nature of the applications and data, the amount of revenue they generate, and the number of users they support. As an illustrative example — compared to the status quo approach to database backup and recovery:

- For *every $10M in annual revenue*, the faster time to recover provided by an engineered systems approach to database protection reduces the annualized business impact of unplanned disruptions by a **median of about $200K**, with a **“long tail” of more than $1.2M**.
- For *every 1,000 users*, the faster time to recover provided by an engineered systems approach to database protection reduces the annualized business impact of unplanned disruptions by a **median of about $40K**, with a **“long tail” of more than $1.3M**.

What Happens Next

What action the senior business leaders in any given organization will take as a result of this analysis is by no means certain. That is, they may decide to *accept* the current risk; *transfer* the risk to another party; or take steps to *manage the risk to an acceptable level*. 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.

For more information, read the full report.

About Aberdeen Group

Since 1988, Aberdeen Group has published research that helps businesses worldwide 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.