Disaster Recovery Is A Business Strategy

A WHITEPAPER BY

[deft]

v21.4

Preface

Disaster Recovery Is a Business Strategy

In today's always-on, information-driven organizations, business continuity depends completely on your IT infrastructures and business processes being up and running 24/7. The costs of downtime are huge, and even minor data loss can quickly put a company out of business.

Since data loss and downtime have direct impact on the financial performance of the business, disaster recovery is an issue that must be based on strategic business criteria and goals.

Business Continuity/Disaster Recovery used to be largely a challenge of natural disasters, power outages, hardware failures, and user error causing data loss. Today, more and more disaster events are declared over software problems and cybersecurity-related threats. Where BC/DR once only focused on technology, it is now equal parts technology, security, and business operations. Comprehensive strategies that minimize data loss and downtime are crucial for modern businesses. As companies become more and more distributed and dependent upon private, hybrid, and public clouds, they must take a comprehensive view of the threat landscape.

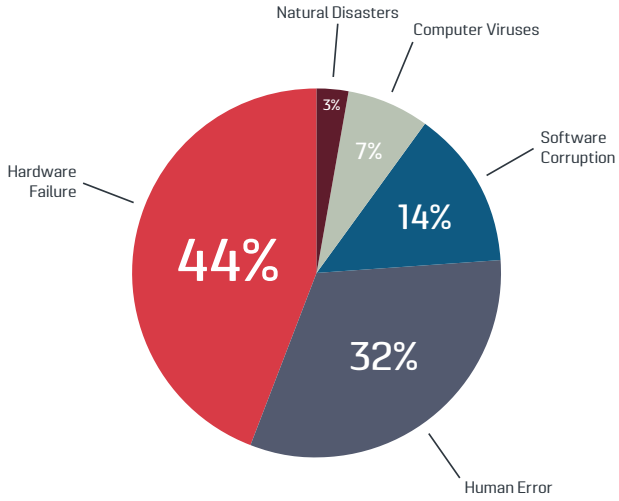
In this white paper, we provide insights into the challenges and strategies available for business continuity and disaster recovery in the cloud era. If reading this leads to any questions, please contact us at sales@Deft.com or visit us at www.deft.com.

www.deft.com / sales@deft.com / +1(312) 829.1111 / 111 W. Jackson Blvd. Suite 1600 Chicago, IL 60604

Disaster Recovery: The Facts

The causes & costs of data loss

Modern businesses can't afford to lose data. Whatever the cause – natural disaster, human error, or cyber attack – data loss is costly and extremely risky. Research from various institutes shows that the volume and costs of data loss are increasing year over year. The need for a business continuity strategy to ensure uptime, diminish data loss, and maximize productivity in the midst of any compromising situation is a necessary digital insurance policy for any company. The question is no longer if a disaster will strike, but when and how.



TOP CAUSES OF DATA LOSS AND DOWNTIME
(source: World Backup Day)

Disaster Recovery in the Real World

Businesses must ask themselves, "How much does an hour of downtime cost?" 95% of companies aren't able to answer this question. Even a simple guess puts you ahead. Then you have to figure out a plan for avoiding that loss.

What Is Disaster Recovery?

DR is the time and labor it takes to resume critical applications and business processes after data loss or downtime.

What Disaster Recovery Solutions Are There?

The most commonly used disaster recovery solution is backups, which involve copying (or replicating) data and applications to another device/location at regular intervals. Backups frequently address compliance requirements for their ability to restore applications and data in the event of a system failure.

Are Backups Enough?

Should an actual disaster event occur, however, businesses often discover that backups are not sufficient. The ability to recover data and applications

typically involves more than copying data back to the original (or comparable) systems. The biggest challenge with backups is when applications must be reconstructed and there is little to no automation built into the backup process. In these cases, backups alone are too weak to address real-world BC/DR and business requirements.

What About Replication?

Replication of data and applications takes backups one step further by introducing failover infrastructure, which provides a more rapid return to normal operations. For critical applications, however, replication restore times can quickly exceed business requirements.

www.deft.com / sales@deft.com / +1(312) 829.1111 / 111 W. Jackson Blvd. Suite 1600 Chicago, IL 60604

...in the Cloud

Many organizations have migrated their applications and platforms to private, public, or hybrid clouds to gain real efficiencies and measurable savings. This opens up great opportunities for the business, but can put your company at even greater risk if people fail to update the BC/DR plan to match the new cloud infrastructure. Too often we hear from companies who had their systems go down, only to realize their BC/DR strategies were based on dated solutions and processes that were not designed for cloud-based environments.

As your infrastructure becomes more complex, so too does your BC/DR planning. Through all the business processes and technologies, you need a consistent and repeatable disaster recovery plan — an increasingly challenging ask.

400%
Growth
Total volume of data loss in two years
(Security Week)

$2.1
Trillion
Total cost of data breaches in 2019
(IT Web)

64%
of companies
Experienced major disruptions in the past 12 months
(EMC)

71%
of IT decision makers
Not confident in their ability to recover
(CIO Insight)

15M
Applications
Deployed on virtualized infrastructures
(CIO Insight)

86%
of all server workloads
Are virtualized in 2016
(Gartner Group)

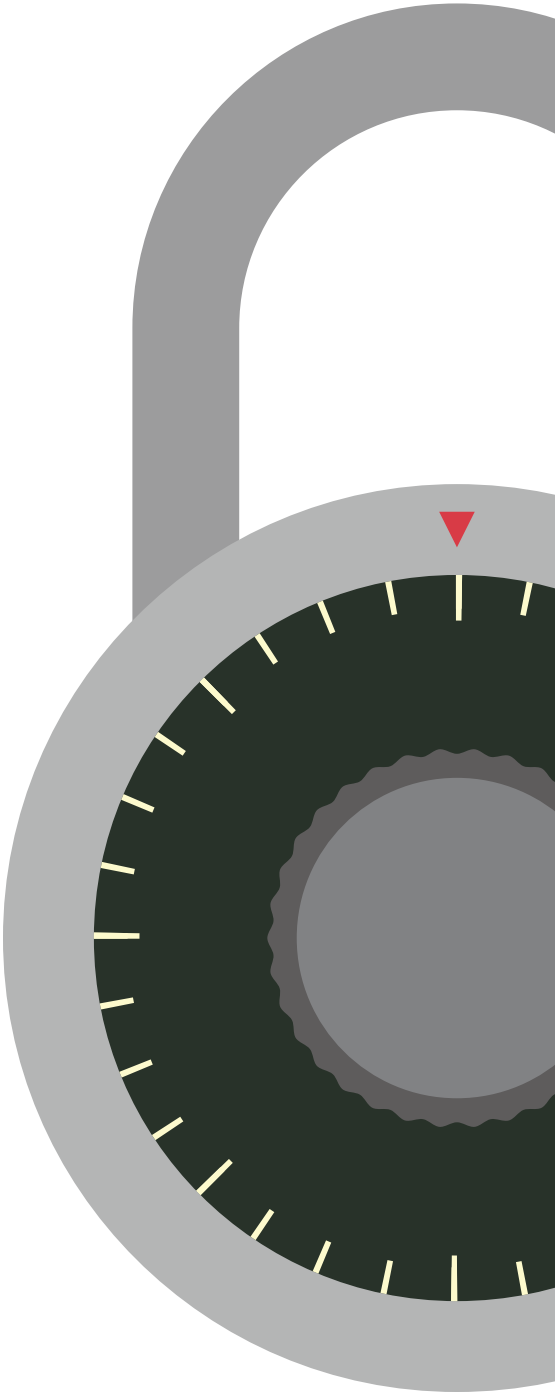
www.deft.com / sales@deft.com / +1(312) 829.1111 / 111 W. Jackson Blvd. Suite 1600 Chicago, IL 60604

BC/DR For Security

Another frequently overlooked benefit to a comprehensive BC/ DR strategy is security. With the rising trends in ransomware, DDoS attacks, phishing, and increasingly sophisticated social engineering hacks, a comprehensive BC/DR strategy can significantly mitigate data loss should a security event occur.

A comprehensive BC/DR strategy — and a proven partner — can augment your security strategy by helping you to:

- Rewind the systems to the last point in time before the infection struck, down to a matter of seconds.
- Recover all the critical systems within the space of a few minutes, with only a few clicks of a button.
- Not only restore entire applications and databases with consistency, but restore individual files as well.
- Perform non-disruptive failover tests at any time, to be sure the business can be brought back online straight away when needed.
- Continuously modify your BC/DR strategies and processes to meet increasingly complex threats and ever-evolving compliance requirements.



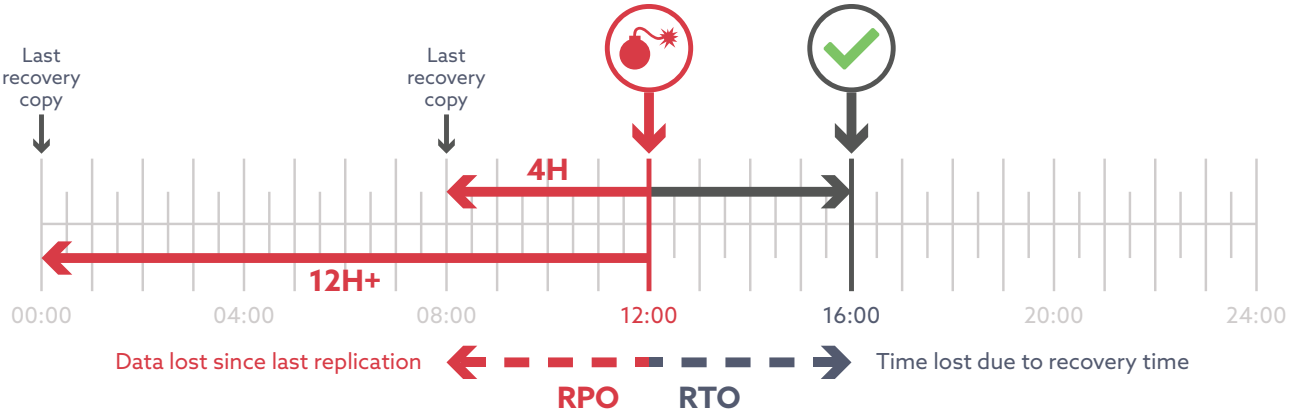
www.deft.com / sales@deft.com / +1(312) 829.1111 / 111 W. Jackson Blvd. Suite 1600 Chicago, IL 60604

Defining Business Continuity

Many companies have a – preferably remote – disaster recovery site where data is replicated to on a continuous basis, ready to be leveraged in the event of an outage. If this disaster recovery site is in a remote location, it can also provide business continuity (BC): the ability for a business to continue to operate after a major disruption, like a fire, power outage, or natural disaster. In case the original site is down, the services on the production site can be run on the DR site. This switching process is called **failover.** Once the normal production site is back up and running, the work that has been done at the disaster recovery site must be replicated back to ensure that all that work is not lost. **The ability to failback applications and data from the DR site to the production site is a critical attribute of a solid disaster recovery solution.**

DR sites used to be a copy of the production site in another office location, but nowadays they are often located at the data center of a cloud service provider, or in the public cloud.

RTO and RPO Explained



Any enterprise with a **stock market quotation** has to comply with rules regarding data security; loss of data will result in loss of revenue, reputation, and shareholder value.

An **online business** that loses four hours of business data might end up with angry customers wondering when their bought-and-paid-for goods are coming

If a **transport company's** systems are down for a few hours, it is impossible to plan deliveries and pick-ups efficiently, which has an enormous effect on revenues that are already under pressure

Complex **robotized production processes** that are down after a hardware or software failure cause enormous loss of productivity and revenue.

www.deft.com / sales@deft.com / +1(312) 829.1111 / 111 W. Jackson Blvd. Suite 1600 Chicago, IL 60604

Once you know the costs associated with downtime, RTO and RPO analyses can be performed to address your unique risk tolerance.

RTO and RPO

When it comes time to translate business needs into Service Level Agreements, recovery is usually expressed in two types of objectives: RTO and RPO.

The **Recovery Time Objective** (**RTO**) is the amount of time the business can be without the service that needs to be recovered, without the service that needs to be recovered before incurring significant losses or risks. The **Recovery Point Objective** (**RPO**) is the most recent point-in-time from which data can be recovered.

Traditional backup or snapshot technologies have RPOs as low as 15 minutes and as long as 24 hours. In modern, ubiquitously digital enterprise environments, both RTO and RPO need to be as low as possible, no longer expressed in hours but in minutes or even seconds. Though many organizations focus on RTO to get the business up and running as soon as possible, it is the inability to reproduce the loss of data (RPO) that will haunt an organization for a long time after any disaster.

High Availability

A concept that is often confused with business continuity and disaster recovery is **high availability** (**HA**).

This is functionality that helps avoid downtime caused by hardware issues. **HA technologies are necessary to keep systems running and performing optimally, but they will not help you recover after a disaster.**

High Availability is most often expressed as a percentage somewhere close to 99%. But don't forget that 99.9% uptime still means that a system has eight hours of unplanned downtime in a year.

High Availability in % and in Time (source: Wikipedia)

Availability %	Downtime Per Year	Per Week
90% ("one nine")	36.5 days	16.8 hours
99% ("two nines")	3.65 days	1.68 hours
99.9% ("three nines")	8.76 hours	10.1 minutes
99.99% ("four nines")	52.56 minutes	1.01 minutes
99.999% ("five nines")	5.26 minutes	6.05 seconds

www.deft.com / sales@deft.com / +1(312) 829.1111 / 111 W. Jackson Blvd. Suite 1600 Chicago, IL 60604

Disaster Recovery Is a Business Strategy

As we've proven, since data loss and downtime have direct impact on the financial performance of the business, **disaster recovery is an issue that must be based on strategic business criteria and goals**.

Questions like how much downtime a business can survive and how much data loss would be acceptable – setting RTO and RPO – are impossible to answer from only a technical level. The answers depend on revenue streams that come from IT systems, the value that is associated with corporate data, logistics, and other business processes that, while heavily dependent on IT, have far broader implications. The bottom line: though a lot of technology is involved, BC/DR is a key element to effectively support business goals and financial objectives.

Deciding What Is Really Critical

When it comes to developing a BC/DR strategy, it is important to realize that not all systems, processes, applications and data are created equal.

For the core applications, a comprehensive BC/DR strategy involving a remote DR site, low RTO/ RPO (short recovery time and low data loss), and a proven, frequently tested recovery plan, is essential.

For other less critical applications and data, less expensive solutions with higher RPO/RTO might be more acceptable as the operating and financial risks are lower.

Prioritization is a key element for disaster recovery planning. Review what downtime can be tolerated for each application with line-of-business owners. We created a simple worksheet to help you get started with prioritizing application recovery. Download it here.

www.deft.com / sales@deft.com / +1(312) 829.1111 / 111 W. Jackson Blvd. Suite 1600 Chicago, IL 60604

DR Is Governance

Finally, many organizations, both large and small, are facing compliance and governance requirements when setting their BC/ DR strategy. As data retention and security regulations continue to increase on a country-by-country basis, the processes and procedures necessary to meet these requirements will continue to increase in complexity.

The question you'll need to be able to quickly and easily answer is: "where is your data stored and who is in control of that cloud platform and data?" Be sure your conversations with service providers include all aspects of your compliance and governance requirements.

BC/DR Is a Financial Decision

There are many ways to design a BC/DR strategy. However, each decision comes with trade-offs. In addition to the financial risk assessment we previously discussed, there are very real financial implications that determine the solutions utilized in your BC/DR strategy.

The most cost effective solution, Backups, will be good enough for many types of applications and data. However, for modern applications, Replication will likely be required. This will increase costs over Backups as it introduces the requirement of a secondary site at another location or cloud-based infrastructure for application and data recovery.

One step further is a comprehensive Disaster Recovery as a Service solution. DRaaS encompasses a complete suite of services that address (and execute) the BC/DR requirements for your organization—all while keeping you in-line with security and compliance requirements via regular business process reviews and system testing.

The cost associated with these solutions will have a material impact on your final strategy. Be sure you're working with a partner who will help you select the right solutions for your business.

www.deft.com / sales@deft.com / +1(312) 829.1111 / 111 W. Jackson Blvd. Suite 1600 Chicago, IL 60604

Additional Questions

For more information, visit www.deft.com or contact us at (312) 829-1111 and sales@deft.com

About Deft

At Deft, we are our clients' most Trusted Advisor.

The Deft team humanizes technology. We actively listen to our clients, learning and collaborating to develop tailored proposals that perfectly fit your company's needs.

We then design, build, operate, secure, and scale unique technology solutions with a singular purpose: to deftly deliver on the promise of technology for you and your customers.

Learn more at www.deft.com or contact us at (312) 829-1111.