

Building the  
business case for  
business continuity  
& disaster recovery  
in small & mid-sized  
organizations

All apps are not  
created equal

A WHITEPAPER BY

*[deft]*

## Introduction

Whether we are supporting our customers in their desire to provide highly available, always-on solutions or helping partners and prospects determine what the right level of continuity is for their business, Business Continuity and Disaster Recovery (BC/DR) are always top of mind for everyone at Deft.

Our goal in putting this white paper together is twofold. First, we'd like to share what we're seeing in and around BC/DR. Second, and most importantly, we hope to provide you with the elements necessary to build a successful business case for your own BC/DR project.

The key to this process? Recognizing that all apps are not created equal.

If you have any questions at all, please do not hesitate to contact us at your convenience. That's what we are here for. You can reach us via email at [sales@deft.com](mailto:sales@deft.com) or call us at 312.829.1111.

## About Deft

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

We know that technology promises the world—streamlined infrastructure, instant scalability, seamless cloud migrations, and much more. We also know technology doesn't live up to its promise without the right partner. This is why we 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.

## What's behind Deft

One question we're often asked at the beginning of BC/DR conversations is, "What's behind Deft?" This is usually a polite way of asking, "You aren't putting my servers in closets with store-bought air conditioners blowing on them, are you?"

The answer to this question is, "A lot!" Deft operates out of the most sophisticated data centers on the planet. These data centers are strategically located on top of major peering points for the Internet. This enables us to deliver unparalleled connectivity and minimize application latency for customers.

Most importantly, each of these facilities is designed from the ground up for reliability across security, power, cooling, and bandwidth, which protect the infrastructure and applications deployed within.

This is important to note because if the data centers housing your infrastructure and applications aren't designed to be in continuous operation, it doesn't matter if your applications are.

## The facts

At Deft we talk to customers, partners and prospects everyday about their business strategies.

We're also constantly watching what's happening in the industry relative to BC/DR solutions and the evolving strategies that keep businesses online — especially in light of the rampant increase in malware and ransomware attacks.

In these efforts, we regularly come across data and insights that completely grab our attention:

**>57%** of small & mid-sized businesses (SMBs) have no recovery plan in place for a network outage, data loss, or other IT disaster.

Obviously we disagree with this, but it was beginning to paint a clear picture.

Something was wrong. Really wrong. We needed to dig even deeper.

At this point we began asking far more detailed and difficult questions about BC/DR. We quickly learned that one of the reasons for this statistic is that business decision makers didn't consistently understand the financial impact of a systems outage. That's a fair enough point. The revenue lost or put at risk by an application or infrastructure outage might not be easily known or quantified for a business. However, not knowing this answer can have dire consequences. So we did what we always do at Deft, we set out to find this answer for them.

Here's what we learned:

# 107 Minutes

The average downtime for a disaster event is 107 minutes. 107 minutes, on its own, doesn't sound like too much time. After all, it's less than two hours. What can happen in two hours?

# \$7,900

Quite a bit can happen in two hours, actually. The average amount of revenue lost per minute of downtime is \$7,900 for mid-sized and SMBs. When you add enterpriselevel organizations into the mix, the value balloons to well above \$20,000 per minute of downtime. All of a sudden, 107 minutes start to matter.

# \$845,300

107 minutes at \$7,900 per minute means that on average \$845,300 is lost per disaster event for mid-sized and SMB organizations. Obviously your mileage may vary based on the size and nature of your organization. However, what's important to note, is that the risk profile for a seemingly "average" disaster event is far more significant than most organizations recognize. After all, as we learned, 52% of business decision makers don't think computer systems are critical to business continuity.

Finally, a bit of icing on the fact cake.

**25%** of mid-sized and SMBs never reopen after a disaster.

**43%** of them never reopen after a catastrophic data loss.

If your organization is lucky enough to survive the first two cuts, the odds are still seriously stacked against you because 75% of SMB and mid-sized organizations who do not have a DR plan are out of business within 3 years of the disaster event.

When you look at all the data, it becomes obvious that understanding BC/DR is critical to an organization's success.

At this point you're probably saying...

"I mean, really, how likely is a natural disaster?"

Here's the kicker. BC/DR isn't about natural disasters. BC/DR is about business continuity.

---

Statistics compiled from the following sources: Business Resumption Planners Association, Forrester Research, Gartner, IDC, Ponemon Institute, Small Business Administration, 451 Research

Here's why:

**60%** of all disaster events are caused by human error

And that's a conservative estimate. Our research, and that of our partners at Zerto, Veeam, and 451 Research, shows this number is 70% or more.

BC/DR is not an insurance policy. BC/DR is about making sure your organization can maintain operation in the face of the day-to-day events that threaten to bring it down.

Something as seemingly insignificant as a power outage or a delayed system upgrade can have very real consequences. It doesn't take long—less than two hours—to lose nearly a million dollars.

## All apps are not created equal

After an organization recognizes the importance of a BC/DR strategy, the next step is to figure out how to put a strategy in place.

The biggest challenge to implementing any strategy is cost. The good news? Here's what we learned:

**Your BC/DR strategy doesn't need to be prohibitively expensive.**

It can even be affordable.

One of the biggest obstacles to achieving a cost-effective BC/DR strategy is many organizations do not know which applications are truly critical to their success.

Whenever we ask, "How many critical applications do you have?" we consistently receive the same answer, "All of them." While "all of them" may be the right answer, a BC/DR strategy for "all of them" may not be necessary, let alone technically or financially feasible.

---

Statistics compiled from the following sources: Business Resumption Planners Association, Forrester Research, Gartner, IDC, Ponemon Institute, Small Business Administration, 451 Research

What our day-to-day work and research has shown us is that all apps are not created equal. The answer to “How many critical applications do you have?” isn’t really, “All of them.” Rather, the answer is, “We aren’t really sure.”

At Deft, we have been diligently studying the answers to these questions in our interactions with our customers, partners and prospects for the past 18 months.

| Applications/Services | Recovery Point Objective (RPO)* |
|-----------------------|---------------------------------|
| Email                 | <10 minutes                     |
| Phones                | <8 hours                        |
| Internet              | <1 hour                         |
| File Servers          | 24+ hours                       |
| CRM                   | <1 hour                         |
| ERP                   | <1 hour                         |
| eCommerce             | <10 minutes                     |
| Development Stack     | 8–24 hours                      |
| Security/Compliance   | <8 hours                        |

\*A Recovery Point Objective (RPO) is the maximum amount of time data might be lost from an application or IT service due to a disaster.

As you can see, there is quite a bit of variance in the importance of these applications and services.

We’re not quite sure why email is more critical than CRM or ERP, other than the emotional impact of not being connected to email, but you get the point. There are wildly varying RPOs on an app by app basis. Obviously, all of these apps are not equally important to the organization’s continued operation and success. Given this fact, why are they continually being addressed as such in BC/DR planning?

This is an easy question to answer. All applications and services are seen as equally important because it’s easy to say, “All of them” vs. looking at each application individually and understanding its importance to the organization.

Let's dive a bit deeper and see how we can apply this data to developing a comprehensive BC/DR strategy.

As you can see, our research has identified multiple RPO windows that consistently come into play. Are these the only RPO windows? No. Not at all. However, they are a great starting point.

From this starting point, we worked with our managed services and cloud teams to identify viable options to deliver these RPO windows.

This is how we identified the recommended BC/DR solution for each RPO window.

## Recommended BC/DR Solutions Per RPO Window

| RPO Windows | Proposed Solution                          |
|-------------|--|
| <1 Hour     | DRaaS                                      |
| 1-8 Hours   | Backup & Warm Recovery Infrastructure      |
| 8-24 Hours  | Backup & On-Demand Recovery Infrastructure |
| > 24 Hours  | Backup & Recovery Infrastructure Plan      |

Apps requiring less than 1 hour RPOs are going to require a DRaaS approach to be sure your business can meet its objectives. It's important to note that a DRaaS environment does not need to be a 1:1 ratio of production to recovery hardware.

Every organization, and application, is unique.

Further research is needed to determine the minimum viable infrastructure to support the app in a disaster event state, but the clarity of knowing how to achieve this objective is the point we're trying to make.

Remember, this exercise is focused on removing the guesswork and placing the emphasis on execution.

As you can see, the proposed solutions to achieve the target RPO windows cascade all the way down to simple backup and recovery solutions when the RPO window is more than 24 hours.

Does this mean there is only one solution for each RPO window? No. It doesn't. Again, we're simply trying to bring clarity to the process, remove guesswork, and focus on execution. We want to make BC/DR a reality vs. a project that's simply too big, too complex, or too costly to tackle.

Let's go back to our initial table highlighting the RPO requirements we've identified in our work.

| Applications/Services | RPO Windows | Recommendation                                |
|-----------------------|-------------|---|
| Email                 | <10 minutes | DRaaS   |
| Phones                | 1-8 hours   | Backup with Warm Recovery Infrastructure      |
| Internet              | <1 hour     | DRaaS   |
| File Servers          | 24+ hours   | Backup with Recovery Infrastructure Plan      |
| CRM                   | <1 hour     | DRaaS   |
| ERP                   | <1 hour     | DRaaS   |
| eCommerce             | <10 minutes | DRaaS   |
| Development Stack     | 8-24 hours  | Backup with On-Demand Recovery Infrastructure |
| Security/Compliance   | 1-8 hours   | Backup with Warm Recovery Infrastructure      |

When you pair these applications and their RPOs with a recommended solution, all of a sudden a comprehensive BC/DR strategy doesn't look that daunting. As you can also see, we're building a fairly complete business case in this process — one that will help set priorities, define investment criteria and, most importantly, help your organization achieve its objectives.

One remaining piece to complete your business case is application prioritization. This ranking of each application and service in terms of restore order is called Restore Priority Order. A simple way to think about it is the tiebreaker when there are multiple applications with the same RPO window.

## Deft App Prioritization Worksheet

We've built a very simple worksheet to help you bring this all together. You can access this worksheet [here](#).

As you can see, by adding Restore Priority Order to the process you can put together a fairly complete business case—one that can properly assess the risk associated with each application.

At this stage, there are two steps that remain:

- Verify the disaster event hardware requirements for each application; and
- Identify the costs for each application's BC/DR infrastructure.

Unfortunately there isn't really a way to continue this process within a document. We've certainly tried, but haven't yet been successful. We've reached the point where it's necessary to get to a whiteboard and work through the final details that will define the total costs of your BC/DR plan.

When you and your organization are ready to take this step, please consider Deft. We welcome the opportunity to work with you through this process, regardless of the partner you choose.

Thank you for reading

### Additional Questions

For more information, visit [www.deft.com](http://www.deft.com) or contact us at (312) 829-1111 and [sales@deft.com](mailto: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](http://www.deft.com) or contact us at (312) 829-1111.