



## A N A L Y S T C O N N E C T I O N



**Phil Goodwin**  
Research Director, Storage Systems and Software

### The Value of Cloud in Lowering Downtime Cost

May 2017

*For the Fortune 1000, the average total cost of unplanned application downtime per year is \$1.25 billion to \$2.5 billion. The average cost of a critical application failure per hour is \$500,000 to \$1 million. Using cloud services for disaster recovery (DR) should be part of an organization's strategy for avoiding the huge cost of downtime.*

The following questions were posed by OneNeck to Phil Goodwin, research director within IDC's Storage Systems and Software practice, on behalf of OneNeck's customers.

**Q. What is the financial impact of downtime on today's enterprise?**

- A. IDC research has shown that the average cost of downtime per hour is \$100,000, though that number can vary greatly by application and organization size. Certainly, there are financial applications that can cost millions of dollars per hour, but the \$100,000 is a good starting number for most organizations to use for planning purposes.

It's important to note that this number is not just for disaster recovery; it also covers all unplanned downtime. IDC recommends as a best practice that organizations quantify their downtime costs, which include productivity, lost business, potential loss of reputation, and the like. The importance of calculating this cost is it can then be compared with the expense of an availability solution. If the cost of the solution is less than the cost of the downtime, then the justification is obvious.

**Q. Why is a disaster recovery strategy a must-have?**

- A. We estimate that nearly half of all organizations could not survive in the event of a disaster due to unrecoverable data loss. This is because systems gradually become outdated, processes become outdated, and suddenly the whole thing is unrecoverable. Disaster recovery is a very complex event involving people, process, and technology.

Too often, IT departments examine only the technology aspect of recovery or, even worse, consider offsite data storage as their DR solution. Good disaster recovery planning lays out in significant detail who needs to do what as well as when and how it needs to be done. Without these detailed plans, organizations that try to recover on the fly face almost certain failure.

**Q. When enterprises are evaluating an on-premises versus off-premises DR strategy, what should they consider?**

A. First, let's distinguish between an on-premises solution and an off-premises solution. An on-premises solution involves two (or more) geographically separated datacenters where infrastructure and workloads are replicated between the two, such that if one goes down the other can take over. These two datacenters are usually under the direct ownership and control of the organization.

The benefit of an on-premises solution is that the IT organization controls the whole thing. There's no conflict for resources with other organizations, there's no resource constraint, and so on.

The downside of an on-premises solution is that it's very expensive. In most cases, an organization needs to double its infrastructure to accommodate full operations in the event of a disaster. Many organizations avoid this because it is so expensive. On the other hand, when we talk about off-premises disaster recovery, we're talking these days about cloud solutions, although there are different models.

Cloud has fundamentally changed the economics of disaster recovery and has made it more affordable for most organizations; instead of buying or contracting for a whole set of redundant infrastructure, organizations can subscribe to base-level services. In the event of a disaster, full infrastructure requirements can be subscribed on demand to fulfill the workload recovery. Cost-benefit analysis should always be calculated, and many organizations are finding cloud DR capabilities compelling, especially when compared with the cost of on-premises.

**Q. What questions should an organization ask a cloud DR provider?**

A. As I mentioned previously, disaster recovery is the combination of people, process, and technology. Those are the three primary areas you need to examine when you are talking with a disaster recovery provider.

First, does the infrastructure capability of the provider support all your workload requirements? You may have physical and virtual infrastructure, you may have iSeries, you may have mainframes. Not all vendors can support all those types of infrastructure.

Second, how can the vendor ensure that your processes are properly documented, such as runbooks, and that they're kept up to date? Again, this is the process part that must be matched with the actual operations.

Third, how can the vendor's or provider's staff help if members of your own staff are unavailable for the recovery? Addressing these three areas will help frame the conversation and make sure all the bases are covered with respect to people, process, and technology.

**Q. What are the current trends or new methods of disaster recovery given the influences of cloud and other technology advances?**

A. Although I have preached that disaster recovery includes people, process, and technology, it's also true that technology, over time, can help replace both people and process. In a disaster recovery scenario, that's a good thing because process and people are where most of the failures occur.

As DR as a service evolves, more technology is being introduced to assist with both people and process. A good example is workload migration, where an entire workload is automatically moved and recovered. And, importantly, this also assists with failback, an area that's often overlooked in disaster recovery planning.

Testing is another area that has seen significant improvement over the years. In many cases, nondisruptive testing tools are available from the provider that can help identify failures without having to actually do a failover. Rather than the old-school annual, massive DR test that took months of planning to execute — and often failed — IT organizations can perform virtual testing with cloud providers as often as they want, making an actual test much smoother.

#### ABOUT THIS ANALYST

*Phil Goodwin is a research director within IDC's Storage Systems and Software research practice. He provides detailed insight and analysis on evolving industry trends, vendor performance, and the impact of new technology adoption. Mr. Goodwin is responsible for producing and delivering timely, in-depth market research with a specific focus on data protection, business continuity and disaster recovery, and data availability. Mr. Goodwin takes a holistic view of these markets and covers risk analysis, service-level requirements, and cost/benefit calculations in his research.*

---

#### ABOUT THIS PUBLICATION

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

#### COPYRIGHT AND RESTRICTIONS

Any IDC information or reference to IDC that is to be used in advertising, press releases, or promotional materials requires prior written approval from IDC. For permission requests, contact the IDC Custom Solutions information line at 508-988-7610 or [gms@idc.com](mailto:gms@idc.com). Translation and/or localization of this document requires an additional license from IDC. For more information on IDC, visit [www.idc.com](http://www.idc.com). For more information on IDC Custom Solutions, visit [http://www.idc.com/prodserv/custom\\_solutions/index.jsp](http://www.idc.com/prodserv/custom_solutions/index.jsp).

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 [www.idc.com](http://www.idc.com)