

# SMART STRATEGIES FOR BUSINESS CONTINUITY

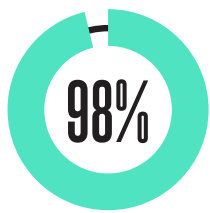
An IT  
Survival  
Guide

7 KILLER QUESTIONS TO ASK YOURSELF ABOUT OVERCOMING  
DATA LOSS & DOWNTIME— AND ENSURING YOUR BUSINESS  
CONTINUITY PLAN DOESN'T EXPLODE IN YOUR FACE

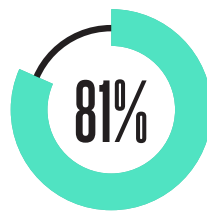
Fear. Bewilderment. Despair. It seems like a nightmare, except it's actually happening in your workplace: you're carrying out your day-to-day IT duties when you're suddenly blind-sided by an unfolding data loss disaster. With spirit-crushing agony, you quickly realize you won't be able to restore your systems soon enough to meet your company's most urgent needs.

It can be a frightful experience—one that threatens everything you've worked for and strived to achieve. Because when you lose data, as all companies will, you can suffer brutal delays in how you do business, lose a fortune in productivity and revenue, and watch helplessly as customers get frustrated by a bad experience and flee elsewhere.

In fact, according to a recent ITIC study,



98% of organizations report that a single hour of downtime costs them \$100,000 or more<sup>1</sup>,



while 81% state that the hourly cost is \$300,000 or more<sup>2</sup>.

And those are just averages: the actual duration and cost of an outage can be far higher, even for small-to-medium sized businesses, often reaching millions of dollars per incidence.

## WATCH OUT—AND BE SURE “DISASTER RECOVERY” APPLIES TO YOUR COMPANY, NOT YOUR CAREER.

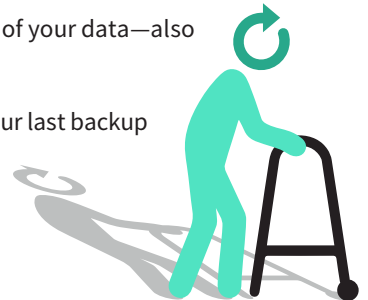
### Standard metrics, substandard results.

Data protection has traditionally focused on two key metrics—RTO (recovery time objective), which measures the time it takes to restore your data, and RPO (recovery point objective), which measures how much data you're willing to lose in an outage.

Over the years, IT professionals have often focused on RTO as the primary way to guarantee a business gets back to normal, to the point where they can now get their data back online lickety-split—doing it in mere minutes, rather than hours...or days.

Problem is solved? Happy ending? Not necessarily. That's because the other key element—the age of your data—also plays a vital role in whether you're able to recover from disaster.

Sure, with your impressive RTO, you may be back up and running in the blink of an eye. But what if your last backup was 10 hours ago, and you therefore can't restore or fulfill any customer orders that were placed during this time span? You'd lose revenue that was already a “done deal,” without ever knowing who placed the lost orders or whether there was a chance of converting them into long-term customers who would provide significant lifetime value. Time to hit the panic button. And tighten up your RPO.





## Budget concerns, a cost-cutting straightjacket.

Of course, in principle, you know your organization needs to establish the RTOs and RPOs that are right for your systems and applications. But budget is always a factor. In terms of RPO, you simply may not have the necessary funds allocated to your IT department to successfully back up all your data as frequently as you recommend. Infrastructure and people costs can gobble up dollars quickly, and limit how many resources you can commit to a backup solution capable of supporting RPOs of minutes.

Unfortunately, to meet these budget restrictions, many organizations are forced to give a back seat to performance. It's a case of the old "penny wise and pound foolish" recipe for disaster. When the purse strings are tightened, you're often forced to settle for backup and recovery tools and methodologies that are inadequate, and that, if left to your own devices, you'd never have chosen in the first place.

## Increasing complexity, non-sustainable status quo.

Perhaps the biggest change in data protection over the past few years is the level of complexity in your IT environment. That's because there are now so many moving parts that confusion and friction are bound to increase, leading to ugly delays in recovery time. Consider the following:



**Variety is everywhere.** Today, you're dealing with on-premises, cloud, hybrid and virtual environments, plus big data, video and photos—all dispersed on mobile devices around the globe. And all of which must be protected, most likely with varying service level agreements (SLAs).



**More backup mechanisms and vendors mean more hassles.** Sure, you may have a great local backup system, but it may not be connected to the cloud. Or your cloud backup may be managed by a different vendor than who handles your data centers. Mobile backups? Look to the individual app providers. And so on, and so on. It's to the point where Gartner reports that average midsize companies have 3+ backup solutions as part of their decentralized operations, with a quarter of these companies looking to switch vendors as soon as possible.



**Data is siloed and unequal.** Given the many environments referenced above, your company's data is probably siloed in many locations—in your data center, in the public cloud, at a remote location, the list goes on. But data is not only separated by where it's housed, it's separated by degrees of importance. You and your IT colleagues had better be able to restore Point of Sale (POS) data in a few minutes, while restoring the presentation from a marketing conference two years ago is a far lower priority. You must be ready to execute a first-to-last action plan when downtime and data loss occurs. Easier said than done—a lot easier.



With so much complexity in today's computing environment, it's fair to say we've entered a new computing era. However, it's likely your business continuity plans were put in place during the preceding era—when the path to data recovery was clearer and simpler.


That puts you in danger. Because if you're still using an old model that assigns a flat dollar value for recovery, without properly determining the actual financial risk of downtime and data loss, you're setting yourself up for failure. Remember, as cited earlier, the average downtime event can cost a midsize company up to \$300,000 per hour or more in direct costs. And that doesn't even include the indirect costs, which include customer turnover and the loss of customer goodwill.



## **BUT WHAT IF WE TOLD YOU THERE WAS A WAY REDUCE YOUR COSTS, REMOVE THE COMPLEXITY AND PREVENT THE CONSEQUENCES OF DOWNTIME ENTIRELY?**

Before exploring how to get there, let's first look at the causes of these disruptions and assess your knowledge of the threats.

Ask yourself the following questions to identify the extent with which your business is at risk, and then we'll show you how to adopt an affordable business continuity strategy that's predictable, sustainable and dependable.



How do you defend against the causes of data loss and downtime—  
and all the devastation they can bring?

## START BY ASKING YOURSELF THESE 7 KEY QUESTIONS— A VITAL FIRST STEP FOR TAKING ACTION.

### 1 Are you burdened by an outdated business continuity plan that leaves you vulnerable to ransomware attacks (they may soon happen every 14 seconds)?

You've heard plenty about them, perhaps even experienced them: Ransomware attacks. They can prove disastrous for your company by blocking you from accessing your own data, and putting you at risk of the losing the data itself.

Without access to your data, you can't fill or track orders. Serve customers. Coordinate sales efforts. Manage your supply chain. Or do any other number of essential business functions. You could even go out of business.

Furthermore, as ZDnet reports, new strains of ransomware are not only holding files hostage, but are being even more destructive—by vaporizing operating system files and requiring a complete rebuild before you can proceed<sup>3</sup>.

Worse, a ransomware attack can hit large enterprises, midsize companies, and small businesses alike. It's no wonder ransomware strains such as WannaCry and Petya strike fear in the hearts of IT professionals around the world. And it's not surprising that the damage is enormous. Cybersecurity Ventures reports that ransomware attacks could cause \$11.5 billion in damage globally by 2019<sup>4</sup>, skyrocketing from the \$2.0 billion in damage that was sustained 2017<sup>5</sup>. And by the end of 2019, it's estimated there will be a ransomware attack on a business every 14 seconds<sup>6</sup>!

That's a scary acceleration in attacks. It shows that the nature of the ransomware threat is growing and mutating quickly. It also begs the question: If your business continuity plan is a few years old, and is in danger of being outdated, is it any match for the havoc that can be wreaked by such the rapidly-evolving ransomware menace?

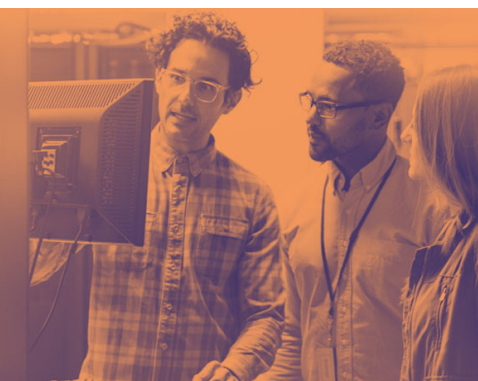




## 2 In the event of a cyberattack, will you be at the mercy of colleagues who are willing to play the “blame game”?

Keeping yourself safe from data loss and downtime is all about having the right data protection. It’s precisely what you need to in order to save yourself from one of the worst threats out there—the cyberattack.

An expertly launched cyberattack can hit you with Distributed Denial of Service (DDoS) on a massive scale—corrupting your devices, making data inaccessible, and rendering you liable to management and customers for security breaches and damages to the victims.



In fact, according to a recent Neustar and Harris survey, a whopping 92% of companies reported that when they experienced a DDoS attack, they also sustained a significant data breach<sup>7</sup>. And even when the DDoS attack is relatively small scale, it can still serve as a smokescreen for a more ambitious goal—to steal data, install malware, map a network’s vulnerabilities, and install ransomware, which, as previously noted, can lead to catastrophic data loss and downtime.

As an example of the danger, consider the healthcare industry, where lives literally hang in the balance when a cyberattack inflicts damage. In early 2018, a hospital in western New York suffered a cyberattack that caused EHR (Electronic Health Record) downtime that lasted two weeks<sup>8</sup>—striking at the core of the facility’s ability to retrieve patient information.

And then there was the case of the large Mid-Atlantic health system that reported 76 medical incidents in the past three years related to downtime (not simply from cyberattacks, but from all causes), disrupting its lab labeling and tracking, medication administration, and ability to provide care without delays<sup>9</sup>.

But even if your industry does not have the life-or-death urgency of healthcare, your career can still sustain significant damage from these types of disruptions: Colleagues may scapegoat you. Angry customers may demand to know “who’s responsible?” And, like many battle-scarred IT professionals, you may even question your own performance. But how do you fight back?

## 3 Will human error reveal a mismatch between your RTOs and RPOs?

Yes, it’s a given that users at your company are the cause of human error. Everyone makes mistakes, with no exceptions—male or female, seasoned or inexperienced, diligent or lackadaisical. Virtually the entire workforce, it seems, is prone to sometimes doing misguided (or just plain dumb or careless) things that can lead to downtime, data loss and data breaches. Even your IT colleagues can be a big part of the problem.

Statistics vary as to how common human error is in today’s office-place, but whether your fellow employees are accidentally deleting a shared directory or folder, making a design or coding mistake, downloading suspect programs or documents, or taking a vanilla milkshake into the server room—the effects can be devastating.

They can also reveal a dangerous disconnect between your RTOs and RPOs. For example, if your servers do get drenched in vanilla, you may have a DR plan that enables you to successfully recover your mission-critical data in only 15 minutes—or, in other words, achieve a 15-minute RTO. You’ll be up and running again fairly quickly.



But does your other key benchmark—your RPO—match the impressive RTO? Is your RPO also timed at 15 minutes, or is it longer, perhaps even hours in duration? The fact is, your 15-minute recovery time won't do you much good if your RPO is 10 hours. You'd be unable to recover any data from customer orders placed during the preceding 10-hour window, and would never know who bought what merchandise or service during that time, or for how much.

In that case, there's a serious mismatch between your RPO and RTO. And yes, the difference may be hidden or seem inconsequential during the uptime of a typical business day. But when a human blunder or any other disaster takes your systems down, the unpleasant truth of the mismatch will be stunningly revealed—and your company will pay the price. (But there is also a solution, as we will reveal.)

## 4 What's a sure-fire way to turn your SLAs to junk? (Hint: Aging technology and dead-end budgets fit the bill perfectly.)



Call it an outdated legacy system. Or a cranky old piece of hardware. Or any other description for ancient relics you can think of. Whichever words you select, aging technology adds a huge element of unpredictability to your operation, often at just the wrong moment, precisely when things (deceptively) appeared to be going so smoothly.

When this old-time technology acts up—and you're forced to endure downtime due to aging server drives, network switches, or any other culprit—you'll find you've got a whole host of problems. Among them, your SLAs may be stretched to the breaking point, and may not be met.

That reflects negatively on you and your entire IT team, no matter how unfair the circumstances may be. All too often, technology professionals like you don't get the share of the budget they need for new replacement resources, but people are sure ready to hold you accountable when a failure occurs.

## 5 Can something as simple as a power outage push your highly complex IT environment over the edge?

It's a fact: Power outages are a growing threat to today's business, as evidenced by the fact that the number of people affected by outages more than doubled between 2016 and 2017<sup>10</sup>, with the average length of an event now at 81 minutes<sup>11</sup>. And while a power outage is often a side effect of a natural disaster (see question #7), it can also be a "solo" event that single handedly takes down the utility company and your organization.



Either way, you'll suffer all the consequences of data loss and downtime, including one that's particularly challenging: Mastering the complexities of an environment that consists equally (or unequally) of on-premise, virtual, cloud and hybrid. Somehow, in this mix, you're expected to get a handle on multiple vendors, varying SLAs, separate silos, far-ranging locations, and tiered levels of data priority—all while making sure the recovery proceeds as planned, and doing it with fewer resources and less time at your disposal.

That's a tall order to fill—whether you're operating in the dark from a power outage, or you're bathed in the cool light of a data center where a downtime disaster is occurring.



## 6 How can breakage suddenly hammer your IT timetables and action plans to pieces?



Things break. Do they ever! And while you may be tempted to blame breakage on aging IT systems (see question #4), the reality is that any element of your IT infrastructure is susceptible to failure, regardless of how long it's been in service.

That's where the problem of sudden breakage comes in—the occasional surprise malfunction. We've all seen numerous examples—for example, a famously-reported instance of a hard drive exploding inside an Exchange server<sup>12</sup>. Witnesses to the explosion heard a crashing and scraping sound coming from the server, which stopped working immediately and caused a 13 day interruption in business operations.

With mishaps like this, it's no surprise that recovery efforts consume such a large portion of your time. It's also clear why it's so difficult for you and your IT colleagues to juggle responsibilities and put out multiple fires simultaneously. How can you plan or operate effectively when a vital piece of hardware goes on the fritz, forcing you into the improvised schedules of “recovery mode” as you stretch your thin resources even thinner?

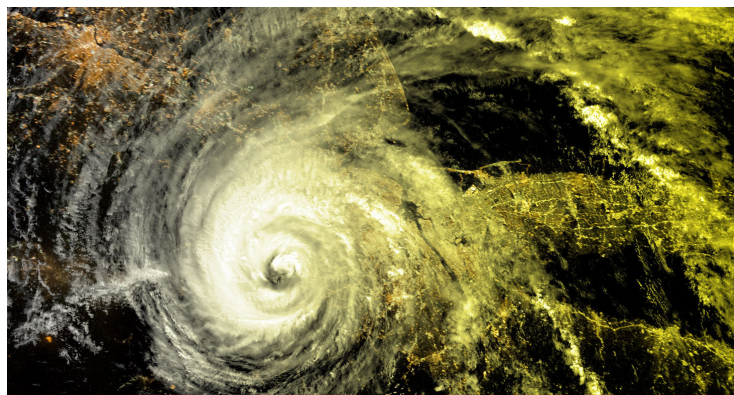
## 7 Last but certainly not least, is a natural disaster the event that will blow away your business continuity plan?

Talk about frightening—the natural disaster is an event that can take many forms: hurricane, tornado, earthquake, fire, flood, or landslide<sup>13</sup>. But whatever form it's in, a natural disaster can wipe out your systems, bury your data beneath a mass of twisted rubble, and cause such extensive damage to your business and the local/regional infrastructure that recovery seems all but impossible.

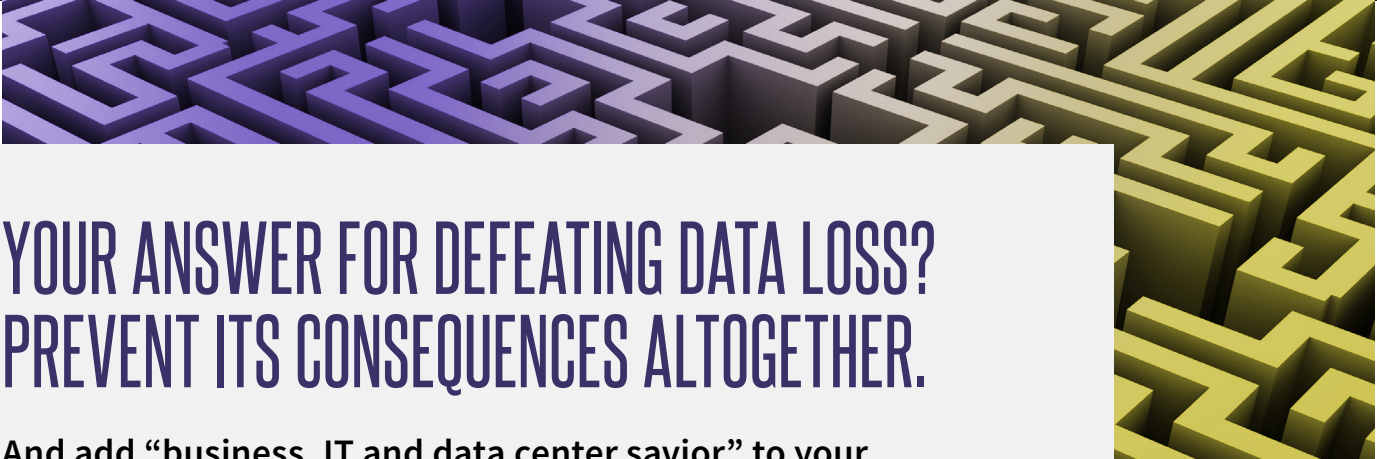
Just look at what happened in 2017, with the brutal 1-2-3 punch of Hurricanes Harvey, Irma and Maria. Or the blazing wildfires in the western part of the U.S. There's every reason to believe natural disasters of this scope will continue in the years ahead, which makes it all the more urgent that your business have a workable, tested business continuity plan.

Problem is, according to our recent survey of IT professionals around the world, over half of the respondents don't have these plans in place<sup>14</sup>. And when they do have a plan, 50% of them test it far too infrequently—only once per year or less<sup>15</sup>. It's no wonder fewer than 15% of these respondents said they had any confidence in recovering their data in the event of a catastrophic data loss<sup>16</sup>.

That's scary when you consider the next natural disaster could be the worst of all—destroying everything in its path, including your plan, unless you're able to put defenses in place that can overcome nature itself.







# YOUR ANSWER FOR DEFEATING DATA LOSS? PREVENT ITS CONSEQUENCES ALTOGETHER.

And add “business, IT and data center savior” to your professional achievements.

As we’ve just seen, it can be difficult to fight back against data loss using today’s data protection methods, particularly given the increased complexity, tougher budget restrictions and higher expectations you find at every turn.

How do you effectively put in place a business continuity plan in this climate? Well, a key step is realizing that the solution isn’t necessarily about recovering from disaster—it’s about preventing the disaster altogether. Think that’s not possible? Think again. Just consider the following:

## Enterprise-level business continuity without enterprise-size budgets.

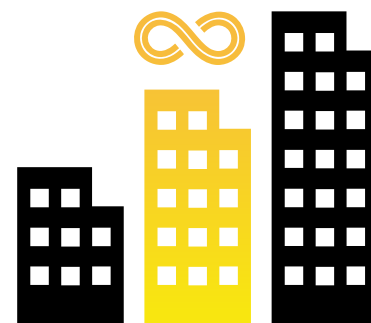
This is one of the most important parts of this eBook. We must first understand the concept of preventing an IT disaster. Rather than cleaning up the proverbial mess that downtime brings, preventing an IT disaster is about reducing the impact of downtime or an outage to a mere glitch from the perspective of your end-users—with an utterly negligible effect on your business.

Better yet, you don’t have to be a large organization to achieve this. Whereas only the wealthiest enterprises used to be able to afford solutions that provided uninterrupted availability and instant recovery, now virtually any size company can prevent an IT disaster. That’s right, your business can achieve the same level of continuity without an enterprise-size budget.

The fact is, the right business continuity solution will do the job for you cost-effectively—reducing an outage to a harmless glitch without the need to over-spend on complex solutions that may not even meet your SLAs for unique systems and applications.

This is a key milestone in recoveries, one in which your business can – and should be taking advantage of. How is this possible?

**We recommend a three-step approach to successfully prevent disasters in your business:**



## Arm yourself:



### Work with your lines of business to develop risk profiles.

Preventing an IT disaster is not just the responsibility of you and your IT colleagues. You need to work with each line-of-business (LOB) team to determine where RTOs and RPOs need to be tight, or where it's permissible to recover older backups of applications. You'll want to collaborate as closely as possible with the LOBs, since buy-in now will avoid problems later.

Specifically, you need to develop risk profiles that describe the level of risk the various lines of business (and your organization as a whole) can tolerate. What data is mission critical and must be recovered immediately? What follows? And after that? It's only by establishing these profiles—and classifying systems and data into levels of priority—that you'll know what's important to recover and how it will affect your operations. Failure to do so can kill your company's resiliency.

Throughout the process, you should be prepared for LOBs to have different ideas on what data is essential. In fact, considering it's only possible for you to serve so many masters at once—and give top priority to only so many systems and applications simultaneously—you may find different LOBs conflict with each other. That's why you need to take a strategic, overarching look at your plan to resolve competing RTO and RPO needs.

## Pinpoint your mission:



### Establish and understand your metrics for business continuity.

First, you need to be realistic about your SLAs. Your SLAs can't stop a natural disaster from occurring, or an especially crafty hacker from breaching your security. But they do provide a guideline for vendors to provide appropriate service, and can serve as legal recourse for you if service is substandard.

When your team is negotiating SLAs, be sure they use your risk profiles as a guide. It's important to understand how disruptions can hurt your business, so you don't over-provision or under-provision the SLAs.

Next, pay special attention to your RPOs. They're often overshadowed by RTOs in today's IT world, but they are absolutely critical to your success. As we've seen, a fast recovery time is always desirable, but if the data was last backed up 24 hours ago, it may be worthless for users of your most important systems and applications.

Suppose you're considering a business continuity solution that guarantees recovery in 15 minutes. All well and good. But to match this tight RTO, what type of RPO can be achieved? Can you also get 15-minute recovery points, and if so, how complex and costly will it be to secure them?

## Stake out the high ground:



### Look to the cloud.

Sixty percent of all IT workloads will run in the cloud by 2019 and by the year 2020, a corporate "No-Cloud" policy will be as rare as a "No-Internet" policy is today. Yet, as we've seen, many organizations continue to use non-x86 platforms, including UNIX, HP/UX, AIX, Solaris and others to support their legacy applications.

With these multi-generational IT environments, businesses face increased risk of data loss and extended downtime caused by the gaps in the labyrinth of primary and secondary data centers, cloud workloads, operating environments, disaster recovery (DR) plans and colocation facilities. Delivering on SLAs is often difficult and protection beyond mission-critical applications and data becomes unrealistic.

To reduce these risks, you need more than bold pronouncements about a new era. You need a solution specifically designed to help you prevent IT disasters in any location, from your systems and applications, on your premises and in your clouds.

To that end, you'll want to leverage cloud-enabled solutions that combine single-service ease of use with a full set of capabilities to restore SLAs and fully protect every single byte in your infrastructure. In doing so, you'll finally be able to untangle the knot of 21st Century IT while supporting RTOs and RPOs – from seconds to hours.



# THE DIFFERENCE BETWEEN IT DISASTERS AND NEAR-ZERO DATA LOSS

As we've covered, the ultimate difference between preventing an IT disaster, or cleaning up after one, comes from determining your risk profiles, pinpointing your business continuity metrics, and streamlining all processes across your distributed, multi-generational infrastructure with one solution that can deliver flexible RTOs, RPOs and SLAs.

Arcserve's Business Continuity Cloud, powered by a unified, cloud-based management interface, puts this reality within reach without being cost-prohibitive or hard to manage. Designed for hybrid multi-cloud infrastructures, it includes backup, disaster recovery, high availability and email archiving to meet your RTOs, RPOs and SLAs without the complexity of dealing with multiple vendors, tools and interfaces. Reclaim your time spent managing backups with a single solution that will:

- **Restore SLAs** and support RTOs and RPOs, from seconds to hours
- **Increase stakeholder transparency** and guarantee system availability with built-in advanced testing and reporting
- **Safely move large volumes of data** to and from the cloud without draining bandwidth
- **Easily scale and pay-as-you-grow** without adding tools or management interfaces
- **Support corporate and regulatory compliance** by simplifying legal discovery and audits
- **Safeguard your IT transformation** with multi-cloud and cross-cloud data protection
- **Prevent downtime and data loss** from complex, multi-generational IT infrastructures with integrated cloud-native, cloud-based and cloud-ready technologies

Serving as “back up your back up,” Arcserve provides an expansive worldwide channel and support network with the expertise, support and resources you need to fully safeguard your business from data and financial disasters.

For more information visit [arcserve.com](https://arcserve.com).



# SOURCES

<sup>1</sup> <http://itic-corp.com/blog/2017/05/hourly-downtime-tops-300k-for-81-of-firms-33-of-enterprises-say-downtime-costs-1m/>

<sup>2</sup> <http://itic-corp.com/blog/2017/05/hourly-downtime-tops-300k-for-81-of-firms-33-of-enterprises-say-downtime-costs-1m/>

<sup>3</sup> <https://www.zdnet.com/article/the-nasty-future-of-ransomware-four-ways-the-nightmare-is-about-to-get-even-worse/>

<sup>4</sup> <https://cybersecurityventures.com/ransomware-damage-report-2017-part-2/>

<sup>5</sup> <https://businessinsights.bitdefender.com/cyber-attacks-how-much-they-will-cost-you>

<sup>6</sup> <https://cybersecurityventures.com/ransomware-damage-report-2017-part-2/>

<sup>7</sup> <https://www.corero.com/blog/846-theft-and-ddos-attacks-go-hand-in-hand.html>

<sup>8</sup> <https://ehrintelligence.com/news/jones-memorial-recovers-from-ehr-downtime-due-to-cyberattack>

<sup>9</sup> <https://www.healthcareitnews.com/news/patient-safety-jeopardized-ehr-downtime-jamia-says#gs.9vbtaEQ>

<sup>10</sup> <https://switchon.eaton.com/blackout-tracker>

<sup>11</sup> <https://switchon.eaton.com/blackout-tracker>

<sup>12</sup> <http://outlookpower.com/article/my-thirteen-days-in-exchange-hell/>

<sup>13</sup> <https://www.zdnet.com/article/diy-it-guide-to-disaster-preparedness-because-its-always-something/>

<sup>14</sup> <https://s13937.pcdn.co/wp-content/uploads/2018/03/WBD-Survey-Results-Infographic-v2.pdf>

<sup>15</sup> <https://s13937.pcdn.co/wp-content/uploads/2018/03/WBD-Survey-Results-Infographic-v2.pdf>

<sup>16</sup> <https://s13937.pcdn.co/wp-content/uploads/2018/03/WBD-Survey-Results-Infographic-v2.pdf>

