Acronis

WHITE PAPER

ROI of Disaster Recovery

How to justify disaster recovery as an investment, not a cost

With the world working from home as a result of the global pandemic this year, hackers are targeting organizations with phishing and ransomware attacks more than ever before. When devices and equipment are outside of IT's regular infrastructure, cybercriminals can more easily find weaknesses to exploit. As such, disaster recovery and business continuity have become even more important topics for many organizations.

According to an ITIC[1] survey, enterprise companies indicate that a single hour of downtime costs their company **over $100,000 a year** on average. The average total cost of unplanned application downtime per year is $1.25 billion to $2.5 billion. Another study by Ponemon Institute[2] found that the average cost of data center downtime was $9,000 per minute in 2019.

If your company is small to mid-size and does not have a sizeable data center, your organization can be at even greater risk. According to the United States Small Business Administration[3], **40%** of businesses don't reopen after a disaster strikes, and **90%** of companies that lose data due to a disaster will shut down within two years. If you don't have a business continuity plan, your company can be a statistic.

Disaster recovery (DR) plans and solutions are a form of insurance. Companies hope that they'll never have to use their DR solution, but they need to protect the business because disasters can happen, and the costs can be astronomical.

As with any insurance policy, you – as a subscriber – will want to calculate the fair price of a premium. You have to weigh the total costs associated with a disaster (if paid for out of pocket) and the likelihood that such an event will occur, against the cost of the "premiums." You are dealing with imperfect information, of course, because you can't predict the future, and can't be sure if, when, and how often you will "file a claim." The best you can do is research case studies and look to best practices for guidance. This document will help you to understand the return on investment (ROI) of a disaster recovery solution.

The need for disaster recovery

Imagine a natural disaster, like any of the more than 200 that occurred across the globe in the first half of 2020. It destroys your office and data center. The owner of the office building has property insurance and will be able to rebuild. The company's employees probably have insurance on their homes and will be able to rebuild as well.

However, what about the business itself? For most companies, data is the most valuable asset: financial statements, customer database, ERP system, emails, etc. When planning for disasters, businesses must ask themselves several questions. "Should we protect our data?" "Can we rebuild without that data?" "How long do we have to rebuild before customers, suppliers, and investors go elsewhere?"

Data can be complicated to rebuild — but it doesn't have to be. It can be copied, stored elsewhere, and made available in a matter of minutes, not in days or weeks — allowing business operations to continue. Traditional insurance might cover new hardware and software, but it can't replace lost data. This is why your organization needs to protect itself by implementing an IT business continuity and disaster recovery strategy.

Despite the risks, some companies do not implement business continuity solutions due to a lack of resources and the difficulty in determining the ROI. This indecision is difficult to comprehend because we understand the value of insurance in other parts of our lives — health, property, life, etc. Why would business data be any less important?

Choosing the right strategy

Every company needs to define its acceptable costs and losses in the event of a disaster:

- **Recovery Time Objective (RTO)** — the time calculated from the moment of the disaster to the moment production operations are back online.
- **Recovery Point Objective (RPO)** — how much data the business can afford to lose, defined by the length of time before the DR event up to the moment the DR event occurs and specified in seconds, minutes, hours, or days. This provides you with the maximum tolerable time that data can be lost.

To determine the RTO, the maximum amount of time that your company can operate without critical systems, you need to analyze the business processes, operations, downtime costs, and available budget. For RPO, your organization may want to preserve 100% of your data — but it may not be economically feasible to do so in every case.

Most companies identify RTOs and RPOs for different parts of the business. For example, the RTO for online customer systems will be much shorter than the RTO for the company's email system. Likewise, the RPO for sales and customer data may be much shorter than the RPO for the email system.

The RPO/RTO combination will help you identify the type of DR solution you will need. For example:

- **For an RTO of 24+ hours,** a cold DR solution is sufficient. In a cold DR solution, you back up your data and keep backup copies off-site.
- **RTO of one hour** will require a warm DR solution. Warm DR means that hardware is ready at a DR facility; however, the operating systems and data are restored after the disaster strikes.
- **RTO of 15 minutes** will require hot DR with ready standby systems. Hardware, operating systems, and data are replicated periodically and are operationally ready on demand.
- **RTO of seconds or zero RTO** will require live, fault-tolerant, long-distance replication.

In general, with shorter RTO, the total cost of ownership (TCO) of the DR solution grows exponentially. It is important to identify and quantify the losses associated with a disaster to estimate the break-even point of downtime versus the cost of the DR solution.

Justifying disaster recovery with return on investment

How do you get your executive team to accept that it is necessary to "insure" corporate data with a DR solution? The best way is to demonstrate that disaster recovery is not a cost — but an investment with a positive ROI.

ROI CASE STUDY: HURRICANE SANDY

In October 2012, Hurricane Sandy caused $70 billion in damages and is still the largest Atlantic hurricane on record. Sandy hit the offices of an Acronis customer on the U.S. East Coast. This customer paid $50,000 per year for an annual subscription with Acronis Cyber Disaster Recovery Cloud to protect all tier-1 and tier-2 servers.

When Sandy hit, the company lost power at its primary data center for three days. In the meantime, the company failed over to the Acronis Cloud and got their servers up and running in approximately two hours. During the three-day power outage, the firm remained operational and productive. The business continued to serve their customers and generate revenue.

If this company had shut down for three days, it would have lost $900,000 in revenues. Instead, the company had used the Acronis solution for about one year, paid $50,000, and saved $900,000 in exchange — that's an ROI of 1700%.

($900,000 Avoided Loss – $50,000 Costs) / $50,000 x 100%
= 1700% ROI

IT IS AN INVESTMENT THAT ANY CFO OR CEO WILL APPRECIATE!

ROI indeed depends on the timing of the actual disaster, the individual business' cost of downtime, and when a DR solution subscription is purchased.

This is why you need to identify the likelihood and frequency of making a "claim." However, when you add up all of the storms, blackouts, equipment failures, human errors, hacker attacks, or conflicts that can affect your IT environment uptime, the frequency of a "disaster" goes up considerably. Many of our customers expect they will fail over part or all of their IT environment once a year.

Let's assume that this same customer had been an Acronis customer for 10 years before the hurricane hit. In that case, their ROI is 80% — still a healthy rate of return.

($900,000 Avoided Loss – $500,000 Costs) / $500,000 x 100%
= 80% ROI

THIS IS EQUAL TO AN ANNUAL RATE OF RETURN OF 10.46%.

To put the 10.46% return rate in perspective, the average annual return for the S&P 500 since its inception in 1928 through 2019 is approximately 10%. However, your CFO will compare the rate of return for the DR investment to other investments and decide whether a return is acceptable. What's important to note is that everything else IT buys depreciates while a DR solution provides a positive rate of return.

There are other economic factors to consider — a strong DR solution will include backup capabilities and address compliance requirements. Most companies acknowledge the need and costs for off-site backups. Thus the focus should be on justifying the additional investment associated with the DR. If your business has compliance regulations, you need to remember to build in the cost risk of the fines and litigation costs related to non-compliance.

Moreover, the implementation of a DR solution may reduce business interruption insurance costs as well. In a BIBA survey[4], "8 out of 10 insurance officers would be willing to provide a premium reduction to companies with a business continuity plan in place."

CALCULATING ROI FOR YOUR COMPANY

You will need to determine several components to calculate a forecasted ROI for your DR solution. The first component is the avoided loss.

- **Unprotected downtime** — the time it will take you to restore company operations without a DR solution
- **Protected downtime** — the time it will take you to restore company operations with a DR solution in place
- **Hourly revenue realized** — divide your company's annual revenue by the number of working hours in a calendar year to get an hourly revenue
- **Determine unprotected downtime loss and protected downtime losses** — multiply both downtimes by the hourly revenue
- **Calculate avoided loss** — you now have the first component of your ROI calculation.

Avoided Loss = Unprotected Downtime Loss – Protected Downtime Loss

The second component of ROI is the cost of your DR solution. Contact Acronis to find out what the DR costs are for your specific environment. Then you'll have all of the components you need to calculate ROI. Before presenting your ROI calculation to your management team, you should ask your CFO for some guidelines on what they consider a good ROI.

ROI = (Avoided Loss – DR Solution Costs) / DR Solution Costs x 100%

CALCULATING ANNUAL RATE OF RETURN

The math for the rate of return is a bit complicated, but the Microsoft Excel RATE() formula can help you. Enter the following formula in your Excel spreadsheet to calculate an annual rate of return. Remember to put the minus sign before the "annual DR solution costs."

= RATE (# of years,-Annual DR Solution Costs, 0, Avoided Loss, 1)

For example, in the previous model, if you input =RATE(10,-50000,0,900000,1) into a cell in an Excel spreadsheet, you get 10.46%.

Conclusion

IT departments seldom justify their purchases using ROI. Instead, many companies make purchase decisions based on savings (hard dollars that are straightforward to calculate) or productivity enhancements (soft dollars that are harder to calculate).

However, when trying to justify a DR solution, an ROI analysis provides the most effective and objective argument for investment. Lastly, remind your executive team of the worst-case scenario. Without a DR solution in place, the company is at risk, especially if the organization is located in geographies prone to natural or human-made disasters.

Next Steps

If you have not yet implemented a DR plan and don't have a solution to support that plan, you should do so immediately. Use the ROI calculation to support your proposal to your management team — and remember to present it as an investment, not a pure cost.

Facing another hurricane or cyberattack without a DR solution in place is unwise. If you need help, contact Acronis for more information.

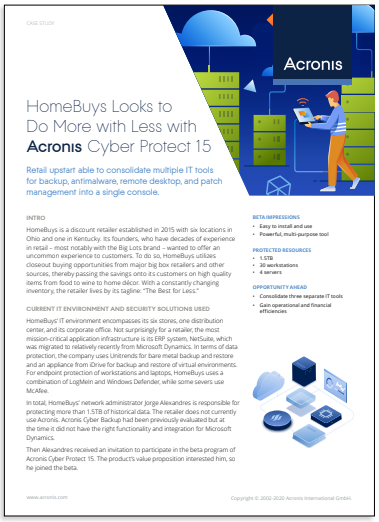
USEFUL LINKS

Acronis Website
Acronis Disaster Recovery Solutions

RESOURCES

[1] "2020 Reliability and Hourly Downtime Trends Survey," ITIC.
[2] "2019 Cost of Data Center Outages," Ponemon Institute.
[3] "Emergency Preparedness," U.S. Small Business Administration.
[4] "The value of business continuity planning," British Insurance Broker's Association.

ADDITIONAL RESOURCES



Acronis Blog: Provides the latest updates and insights from the world's cyber protection leader.

Acronis YouTube Channel: Delivers frequent videos of use cases, demos, cyberthreat analysis, and company news.

Acronis Resource Center: The go-to hub for cyber protection white papers, e-books, in-depth articles, tutorials, infographics, etc.

Acronis Events: Ongoing series of events, webinars, interviews, etc., including details on joining.

ABOUT ACRONIS

Acronis unifies data protection and cybersecurity to deliver integrated, automated cyber protection that solves the safety, accessibility, privacy, authenticity, and security (SAPAS) challenges of the modern digital world. With flexible deployment models that fit the demands of service providers and IT professionals, Acronis provides superior cyber protection for data, applications, and systems with innovative next-generation antivirus, backup, disaster recovery, and endpoint protection management solutions. With award-winning AI-based antimalware and blockchain-based data authentication technologies, Acronis protects any environment – from cloud to hybrid to on-premises – at a low and predictable cost.

Founded in Singapore in 2003 and incorporated in Switzerland in 2008, Acronis now has more than 1,500 employees in 33 locations in 18 countries. Its solutions are trusted by more than 5.5 million home users and 500,000 companies, including 100% of the Fortune 1000, and top-tier professional sports teams. Acronis products are available through 50,000 partners and service providers in over 150 countries in more than 40 languages.

Acronis

Learn more at
www.acronis.com