Acronis

ROI of IT DISASTER RECOVERY

In light of recent U.S. disasters, such as Hurricane Sandy and Katrina, disaster recovery and business continuity are now important topics that are top of mind 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.

Another study by Emerson Network Power and Ponemon Institute [2] found that the average cost of data center downtime was **$7,908 a minute** in 2013 — that is **$690,204** per outage. In addition, 91 percent of data centers experienced an unplanned outage over a **24-month period**.

If your company is small to mid-size and does not have a sizeable data center, your organization can be at an even greater risk. According to the Institute for Business and Home Safety [3], an estimated **25 percent of businesses** do not reopen following a major disaster. If you do not have a business continuity plan, **your** company can be a statistic.

[1] "2013-2014 Technology Trends and Deployment Survey," ITIC.

[2] "Understanding the Cost of Data Center Downtime," Emerson Network Power and Ponemon Institute.

[3] "Emergency Preparedness," U.S. Small Business Administration.

Disaster recovery (DR) plans and solutions are a form of insurance. Companies hope that they will never have to use their DR solution, but they need to protect the business because a disaster 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 compare the total costs associated with a disaster if paid for out of pocket and the likelihood that such an event will occur in relation to the cost of the "premiums." You are dealing with imperfect information, of course, because you cannot predict the future, and cannot 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 the recent wave of tornados that hit the U.S. Midwest, which destroys your offices 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 they will be able to rebuild as well.

However, what about the business itself? For most businesses, data is its most valuable asset: financial statements, the customer database, ERP system, emails, etc. In the event of a disaster, businesses must ask themselves several questions. "Should the business protect its data?" "Can the business rebuild without that data?" "How long does the business have to rebuild before customers, suppliers, and investors go elsewhere?" Data can be very difficult to rebuild — but it does not have to be. It can be copied, stored elsewhere, and made available in a matter of minutes, not in days or weeks — so the business can continue. Traditional insurance might cover new hardware and software, but it cannot replace lost data. This is why your organization needs to protect itself by implementing an IT business continuity and disaster recovery strategy.

In spite of the risks, some companies do not implement business continuity solutions due to 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 the acceptable costs and losses in the event of a disaster:

- The Recovery Time Objective (RTO) — the time calculated from the moment of the disaster to the moment production operations are back online.
- The 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, specified in seconds, minutes, hours, or days. This provides you with the maximum tolerable period of 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 percent 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 a RTO of 24+ hours, a cold DR solution is sufficient. For a cold DR solution, you back up your data and keep backup copies offsite.
- RTO of 1 hour will require a warm DR. A warm DR solution 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 stand-by 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 in order 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 insuring corporate data with a DR solution is necessary? The best way is to demonstrate that disaster recovery is not a cost — but an investment with a positive ROI.

ROI Case Study: Hurricane Irene

In August 2011, Hurricane Irene 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 Disaster Recovery Service to protect all tier-1 and tier-2 servers.

When Irene hit, the company lost power at their main 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 used the Acronis solution for about one year, paid $50,000, and saved $900,000 in exchange — that is an ROI of 1,700%.

($900,000 Avoided Loss - $50,000 Costs) / $50,000 x 100% = 1,700% ROI

This is an investment that any CFO or CEO will appreciate!

It is true that ROI depends on the timing of the actual disaster. This company experienced a disaster just one year after subscribing to Acronis' services, but remember that the timing of when to buy a DR solution is an intelligent guess at best.

This is why you need to identify the likelihood and frequency of making a “claim.” Hurricane Irene was a once-in-a-generation storm. However, when you add up all 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 us assume that this same customer had been an Acronis customer for 10 years before the hurricane hit. In that case, their ROI is 80 percent — 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 percent.

To put the 10.46 percent return rate in perspective, the average annual return for the S&P 500 since its inception in 1928 through 2014 is approximately 10 percent. However, your CFO will compare the rate of return for the DR investment to other investments and decide whether a return is acceptable. What is important to note is that everything else IT buys depreciates while a DR solution provides a positive rate of return.

There is also another economic factor to consider — a well-thought DR solution will include backup and archiving capabilities. You could retire your current backup and archiving products and shift this budget over to disaster recovery. The $50,000 per year for the Acronis Disaster Recovery Service could be a net-zero change to the overall IT budget.

Moreover, the implementation of an IT DR solution may reduce business interruption insurance costs as well. According to a BIBA survey, “62 percent of respondents said that those with [business continuity] plans benefited from premium discounts and reduced excesses [deductibles]. Insurers supported this too, with 83 percent of those asked saying that they would provide a discount or improved insurance terms to a business interruption policy if a business continuity plan was in place.”

Calculating ROI for your company

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

- **Unprotected downtime** — how much time will it take you to restore company operations without a DR solution
- **Protected downtime** — how much time will it 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. You can contact Acronis for the costs of DR services for your environment. Now you have all 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 he/she considers 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. Simply enter the following formula in your Excel spreadsheet and it will give you 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 example, if you input *=RATE(10,-50000,0,900000,1)* into a cell in an Excel spreadsheet, you get 10.46 percent.

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 hard 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, as a going concern, is at risk especially if the organization is located in geographies at risk to natural or man-made disasters.

Next Step

If you have not yet implemented a DR plan and do not 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, typhoon, tornado season, earthquake, or conflict without a DR solution in place is irresponsible. If you need help, contact Acronis for more information.

USEFUL LINKS

Acronis Website

Acronis Disaster Recovery Service

ABOUT ACRONIS

Acronis sets the standard for new generation data protection through its backup, disaster recovery, and secure access solutions. Powered by the AnyData Engine and set apart by its image technology, Acronis delivers easy, complete and safe backups of all files, applications, and OS across any environment — virtual, physical, cloud, and mobile.

Founded in 2003, Acronis protects the data of over 5 million consumers and 300,000 businesses in over 130 countries. With its more than 100 patents, Acronis' products were named best product of the year by Network Computing, TechTarget, and IT Professional and cover a range of features, including migration, cloning, and replication.

For additional information, please visit www.acronis.com.
Follow Acronis on Twitter: http://twitter.com/acronis.

For additional information, please visit www.acronis.com

To purchase products, please visit http://www.acronis.com/en-us/company/contacts.html#international to find an Acronis office or authorized dealer.