EVOLVE IP
THE CLOUD STRATEGY COMPANY™

Cloud Brief

Blindsided by an Outage: An Executive Primer on Disaster Recovery and Business Continuity

This cloud brief explores the frequencies and costs of downtime, the essential elements of Disaster Recovery and Business Continuity (DR/BC) and the critical need to view disaster planning as a fundamental aspect of your business strategy.

Introduction

Virtually every company is at risk of a disaster that could bring productivity to a halt. Disasters can be caused by unpredictable events, such as fires and hurricanes, but human error and cyberattacks *(see sidebar)* are also common causes for disrupting productivity, reputation and profitability. Even worse, according to the Institute for Business and Home Safety, an estimated 25 percent of businesses do not reopen following a major disaster. This is why comprehensive business continuity (BC) and disaster recovery (DR) planning is essential.

BC planning ensures that organizations can continue to operate in the event of a serious incident or disaster. Meanwhile, DR planning focuses on storing data so that it can be accessed following a disaster, enabling organizations to become operational within a reasonable timeframe after a system failure. Business continuity takes data storage into account, but also focuses on the risk management, oversight and planning an organization needs to stay operational during a disruption.

Widespread Liabilities

According to the Evolve IP 2018 Survey on Disaster Recovery, more than one-third of nearly 1,000 executives and IT professionals reported at least one incident or outage that required disaster recovery mitigation. And, of those that experienced a disaster, 42.5 percent suffered disaster recovery events more than once.

Let's put a face to these numbers. In August of 2016, thousands of travelers were stranded after a Delta airline systems outage. The outage, caused by server failure in the data center, resulted in 2,000 flight cancellations over a three-day period. This outage cost Delta $100 million in lost revenue, and it damaged the company's reputation.

Is Your Business Ready?

Data shows that business leaders tend to believe they're better prepared, as they typically don't have a granular view of their technical capabilities to survive disasters and resume business after an incident. Meanwhile, most IT professionals are better versed in the risks, and have a less optimistic outlook. In fact, 47 percent of technology professionals believe they are just "somewhat prepared" to recover in the event of a disaster, and the vast majority have just an "incomplete" disaster recovery plan. In many instances, executive leadership is blindsided by the downtime, and the end result is lost revenue and significantly diminished productivity.

TOP SEVEN CAUSES OF DOWNTIME

Hardware failure / Server issues: 50%
Environmental disasters: 29%
Misc. power outages: 28%
Human error: 18%
Software failure: 18%
Deliberate attacks: 17%
Backup / restore failure: 10.5%

Source: The 2018 Disaster Recovery Technologies Survey

The Cost of Downtime

To begin estimating your liability, make an appraisal of downtime costs and potential losses. Whether a disaster is caused by an accident, employee-sabotage, hacking/ransomware or weather, it's important that you understand the financial implications of an incident. The completion of a specific business impact analysis will reveal your organization's true costs of downtime, and executives will be better able to work with technology leaders to build an effective plan and reduce the potential of future downtime.

As you calculate the cost of downtime for your organization, consider the following:

- Number of employees
- Average employee wages per hour
- Average % of lost productivity
- Total labor cost per hour
- Gross Annual Revenue
- Days per year / hours per day open for business
- Total revenue lost per hour
- Total hourly downtime cost
- Total downtime cost

EVOLVE IP
THE CLOUD STRATEGY COMPANY™

Cloud Brief

COST OF DOWNTIME
Have you quantified the cost of downtime for your organization? Our straightforward and free calculator gives you a practical option to quickly determine your estimated cost of downtime in consideration of investments in Disaster Recovery and Avoidance solutions. Calculate now: Cost of Downtime Calculator

Building a Plan

Structure your disaster recovery plan based on your entire business, not just your data. It's all about people and productivity. The key to business continuity and disaster recovery planning is deciding which functions are essential – and must be recovered first – and allocating the available budget accordingly. Once crucial components have been identified, failover mechanisms and rapid recovery plans can be put in place.

When identifying priority systems, don't think about types of data. Instead, consider the length of time without access to data. Businesses in a high-transaction environments, such as financial institutions and online retailers, would have an acceptable downtime of next to zero, whereas a small art gallery might operate longer without access to data.

Consider these factors when building your disaster recovery and business continuity plans:

- How do your employees access technology?
- Which compliance requirements apply to your business?
- What are your business priorities: Which systems or data would need to come up first?
- How many geographic locations will be involved, and what are the varying conditions and requirements for each?
- How will future plans impact disaster recovery i.e., new locations, expanded workforce, transitioning to a mobile workforce?

Financial Strategies

When building your plan, consider the costs and how they will affect the bottom line. In an increasing number of instances, business leaders are moving technology expenditures from capital expenses (CapEx) to operational expenses (OpEx). OpEx-based strategies allow businesses to pay only for the needed technologies, versus making significant investments in bloated systems that become obsolete in a matter of months.

This strategy can be executed through cloud-based DR and BC solutions, which provide OpEx benefits, versus purchasing and overlaying disaster recovery solutions into an infrastructure on-premises, which also typically take longer to restore data.

Conclusion

The odds are high that your business is going to have to recover from a disaster. While big disasters can be devastating to a business, little disasters happen every day. Effective disaster planning should be viewed as a fundamental aspect of your business strategy, not just an afterthought. By determining your degree of readiness, including the cost of a potential disaster, you can begin building an effective and financially responsible plan that reduces liability and ensures greater business continuity in the event of a disaster.

Evolve IP's client and analyst-acclaimed disaster recovery suite protects your data and allows you to recover your environment based on how your business runs and the way your infrastructure is designed. From fully managed DR to self-managed solutions to essential cloud backups we have a service that enables IT resilience and fits your recovery timeframes, budget and compliance needs.

We don't shoe-horn clients down a single path. Utilizing industry-leading replication technologies, Evolve IP can create, manage and test resiliency or, provide self-service solutions from Zerto, Veeam, VMware, Nimble / HPE and Double-Take that meet nearly any RTO / RPO. Our extensive suite even extends to recovery for Desktops and for Voice for the most comprehensive approach to disaster recovery and business continuity.

To learn more about Evolve IP's suite of DR solutions visit *www.evolveip.net/draas-suite*.