arcserve®

REPORT

Responding to Downtime:
Five Key Strategies to Know Now

Responding to Downtime:
Five Key Strategies to Know Now

The data protection space keeps evolving as organizations weather the "perfect storm" of challenges currently hitting their IT infrastructures. This "storm" affects the ability of IT teams to effectively run operations, and places economic decision makers in a quandary when allocating budgets. It's no surprise that many IT leaders are kept awake at night with a laundry list of concerns:

- Never-ending growth of structured and unstructured data
- Explosion of malware/ransomware attacks
- Increased requirements to demonstrate compliance and data stewardship
- Inconsistent data protection infrastructures for larger end-users
- Added complexity caused by the combination of loosely integrated solutions
- Lack of control over key metrics, such as RPOs and RTOs
- Eruption of virtualization and the role of cloud-based storage

To compound these challenges, many organizations are putting the burden of managing complex IT solutions squarely on the shoulders of an IT generalist – many of whom require less complex and lower cost solutions to protect, manage and access critical data. It's because of this that organizations need to re-think five key strategies that can either make or break their ability to respond during downtime.

1 | **Risk management:** Actuarial strategy meets data protection

Most organizations today are mandated (or in the very least, heavily encouraged) to have disaster recovery or data availability plans in place. But many of these plans were built in a different computing era, and don't address the return on investment (ROI) and actual cost savings that IT business leaders need when evaluating their current investments. That's where actuarial strategy meets data protection.

Today's organizations need to be able to access critical data – when and where it's needed. Every time an IT leader improves the resiliency of the IT infrastructure, the business realizes cost savings, a significant reduction in risk/loss, and improves operational efficiency. The reason is derived from the economics of backup and recovery, or more specifically, the cost of application and data availability which can be quantified by measuring both direct and indirect costs, such as: reputational impact, loss of customers or their inability to make a purchase, fines when regulatory situations occur and employee productivity. By taking a more actuarial approach to data and system availability, you can determine:

- The loss expectancy based on statistical probability
- How a natural disaster would affect current resources and the cost to get back up and running
- The risk of malware/ransomware affecting critical systems, and the cost and length of time it would take to get data back by either paying or not paying a ransom

- How the business would be able to provide its products and/or services, and what processes are necessary to ensure employee productivity wouldn't decline or the volume of sales wouldn't be affected
- The monetary effect of a POS or e-commerce site going down for five minutes, 15 minutes, or longer. Depending on the sales model, losing the ability to transact online for more than a few seconds can mean a massive loss of business

This actuarial, or more economic approach to backup and recovery, allows an organization to build a model that puts a real number on risk and the incidental loss expectancy costs. In turn, the business can more effectively prioritize the most critical areas of weakness and allocate its investments accordingly.

2 | System Availability: Not all data is created equal

It's common knowledge that most, if not all businesses, wouldn't function without email or critical transactional applications - those that literally run the business or allow customers to purchase products and/or services. It also doesn't take a rocket scientist to understand that protecting these systems and data is key to surviving unplanned downtime. That said, there's a lot more than meets the eye given that these systems and applications are almost always intertwined – more or less successfully - and will have different levels of criticality. As executive teams review their current and future availability strategies, it's important to consider a few key areas:

- The criticality of specific applications: When it comes down to it, the real question should be, "how fast do you need to access specific data?" Marketing brochures and internal file-sharing applications can typically withstand a few hours of downtime, while transactional systems are often mission-critical and must be available in seconds. The financial impact to specific systems can be modeled with the risk management approach mentioned above
- Application and system interdependence: Typically, most applications are combined or integrated in a value chain or workflow, for example EDI orders that feed an entire supply chain. Adding to this complexity is the fact that these applications are commonly monitored in silos, impacting performance and making it harder to manage the entirety of the infrastructure. How would the impact of one system going down affect the others? It's important to understand the extent of interdependence within your organization and the resulting impact to the entire IT ecosphere
- Maintenance schedules and availability: Each application has different maintenance schedules and service level requirements. Based on these, it's important to determine how quickly you'd be able to access specific mission-critical data. Many solutions are more or less "one size fits all," require forklift upgrades or the addition of other point solutions as business needs evolve. Keep this in mind when forecasting future dependencies or changes to your infrastructure

By considering these key areas, you can determine your data availability index and any potential gaps in the workflow or value chain of the applications that run your business – and act accordingly.

3 **Complexity:** More processes, more problems

The earlier points on data availability have unearthed the true culprit in preventing organizations from achieving efficient business continuity: the complexity of the IT infrastructure, and more precisely, of its data protection solutions. The challenge, and subsequent main goal, is to obtain a level of predictability and consistency of recovery, regardless of the interruption event that will inevitably hit every infrastructure. IT leaders and business executives need to approach this challenge from a net result perspective; considering actual RPOs and RTOs, and determining how to get the business back on its feet in a timeframe that meets business requirements. Specifically, this means orchestrating the recovery or failover of critical systems in a way that produces predictable results.

Unfortunately, this is nearly impossible if a business uses multiple backup solutions or discrete processes that are not well orchestrated. Unifying your data backup, recovery and availability infrastructure, whether on-premise or with the help of cloud destinations, is the only way to successfully test your plans and guarantee effective execution should an interruption event occur. Ultimately, the less complexity that's introduced in backup and recovery processes will give you more control over RPOs and RTOs.

[1]http://finance.yahoo.com/news/victims-paid-more-24-million-222700088.html

[2]https://www.justice.gov/criminal-ccips/file/872771/download

4 **Ransomware:** It's not a security issue, it's a data recovery issue

The Internet Crime Complaint Center reported that last year alone, ransomware events cost U.S. organizations $24 million[1], and according to the Department of Justice, ransomware attacks have increased 300% so far in 2016[2]. These statistics underscore a growing issue that's impacting businesses of all sizes; one which company executives cannot ignore, and will inevitably fall back on IT to resolve.

Unlike other logical data interruption events, ransomware can also come with a very high reputational impact. One look at the recent incident involving Delta Air Lines illustrates not only the high cost of ransomware, but the impact of customer trust – which is often the most detrimental result.

The best strategy to mitigate the damage from a ransomware event is to be proactive, instead of reactive. By giving your organization room to make its own decisions, you remove the need to negotiate with hackers should ransomware spread and infect business-critical data. An extremely effective way to accomplish this is by implementing and regularly testing a robust recovery solution with traditional and cloud-based options that enable you to "turn back the clock" and restore business-sensitive data – no ransom needed.

In a majority of ways, the onslaught of ransomware is the biggest threat to organizations today; however, it offers businesses one thing: the opportunity to re-assess business continuity and disaster recovery strategies to ensure no area has been overlooked. By combining a solid threat detection and malware eradication solution with a robust data availability plan, organizations are well positioned to overcome a ransomware event, and the myriad of damages it can cause.

5 Leveraging the Cloud: How and when it makes sense for your infrastructure

Much has been written about using cloud services to supplement or even replace traditional backup and recovery infrastructures, however there are many considerations to address when assessing how and when to introduce a cloud component. Among these, IT and business leaders need to consider:

- The actual type of service, whether it be Backup as a Service (BaaS), Disaster Recovery as a Service (DRaaS) or data/workload hosting
- How you evolve from an on-premise business continuity/disaster recovery solution to a more hybrid infrastructure, including the type of cloud storage (disk, tape or a combination), if archiving will be required, the data ingest and recovery mechanism (how will you get your data to the cloud and back again), and cost flexibility

More importantly, these considerations need to be addressed in the context of the original RPO and RTO requirements. Additional areas of discussion include the provider's facilities and locations, which are to be carefully considered both from a compliance standpoint as well as from a potential disaster impact zone (for example, having data and failover systems located "out of region" is a best practice).

Conclusion

Most organizations understand the urgency in maintaining system resiliency and guaranteeing data availability in the face of continuously evolving threats. Fundamentally, it really comes down to resolving one complex equation: what service levels do I need from a RPO and RTO perspective, and what investments should I make to get those results and maximize return on investment.

Organizations that leverage strategies around risk mitigation, proactive ransomware response, data availability for system ecospheres, processes simplification and the role of cloud, will be well positioned to meet any business demand. So while the "perfect storm" that's hitting many IT infrastructures is certainly a cause for concern, it also represents an opportunity to make business continuity and disaster recovery a meaningful executive-level conversation; effectively shifting the discussion of data loss from being solely an IT concern to a business concern.

For more information on Arcserve, **please visit** arcserve.com