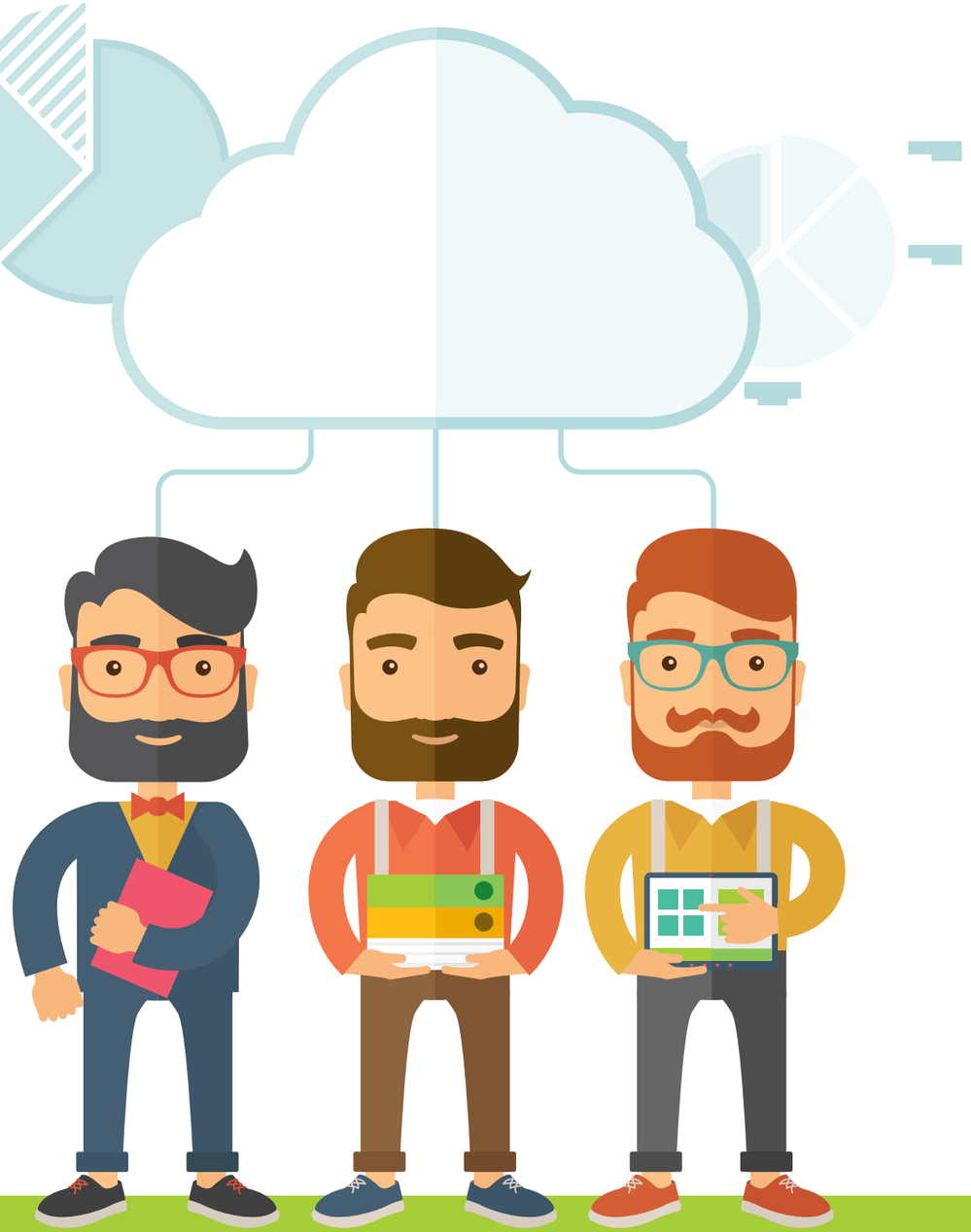
The 5 Downtime Strategies You Need to Change

Quorum®



Ours is the world that never sleeps. Whether your organization performs spinal surgery, designs software or builds bridges, your services are expected to be available whenever they re needed. Websites are expected to always perform at full power, accounts are expected to always be available and transactions are expected to work smoothly at any hour of the day or night.

But while the expectations for continuity and availability are higher than ever, most organizations aren t able to deliver. From hurricanes to cyber attacks to staff errors, downtime can bring business to a halt while damaging brand reputations.

For many IT teams, this demand for continuity has become their #1 challenge. The data protection strategies that were sufficient ten years ago no longer meet their RTO's. They're asked to intelligently allocate their budgets and resources for efficient operations while creating innovations that move their business forward all while keeping the lights on no matter what.

Traditional backup and disaster recovery strategies have hamstrung many teams, demanding they spend too many hours babysitting backups and handling administrative tasks. Many organizations are stuck with recovery windows of two hours or more, saddling their organization with the appearance of incompetence.

An effective BDR strategy addresses security needs, data storage, disaster recovery, backup management and mission-critical systems. It also accounts for the intersection of data management and business initiatives. By adopting a holistic view of downtime, an intelligent BDR ecosystem addresses all of the factors involved, such as:

- Ransomware and other malware attacks
- Ever increasing amounts of data
- Multi-vendor solutions that aren t always integrated smoothly
- The role of virtualization and the cloud
- Meeting complex compliance requirements
- The right data protection strategies for enterprise
- Achieving ideal RPOs and RTOs

The above are challenges common to most teams, yet leaders still struggle to find effective obvious solutions. Often they assign their BDR endeavors to IT generalists who just aren t equipped to navigate complicated solutions or the increasing budget consumption. Other leaders settle for outdated solutions that prove themselves inadequate after a flood or server failure or ransomware attack.

72

SEVENTY TWO

72% of organizations say recovery speed is very critical. Yet over 80% take over an hour to recover from a server failure and more than a quarter need 2 hours or more.[1]

[1]Quorum State of Disaster Recovery Report, 2016

The chief obstacle to success isn t a natural disaster or malware, though it might seem it. The downfall comes from 5 downtime strategies that hinder their ability to run a powerful and cost-effective BDR system.

INEFFECTIVE STRATEGY #1: IGNORING THE ECONOMICS OF BACKUP AND RECOVERY

Organizations often pat themselves on the back for having a disaster recovery or incident response plan in place. And it s true that plans are important. The problem? Many of these plans were constructed before today s complexity, threats and technology. When disaster strikes, gaps in the plan result in more chaos and missteps.

These plans often focus on uptime, as they should. However, they tend to omit important aspects like the return on investment (ROI) and cost savings gained with a BDR solution. Engineers may think in terms of deflecting threats, securing data and keeping servers running, but their leaders view technology as investments which means a good working strategy must factor those equations into their BDR strategy.

By conducting a risk assessment and calculating the cost of downtime, you ll have an idea of the loss expectancy your strategies need to prevent. Include this criteria as you evaluate prospective BDR solutions. Downtime isn t only measured in minutes and hours, but dollars. Basing your backup and recovery strategies on actual numbers of loss expectancy and prevention will help get executive buy-in and ensure your critical resources have adequate protection.

QUANTIFYING THE ROI OF BDR

When calculating the cost of downtime and a good BDR solution savings, consider:

Will automated testing and other features improve operational efficiency?

Does the improved resiliency of the IT infrastructure equal cost savings?

Will backup encryption and improved security reduce risk?

How many lost transactions would be saved?
Employee productivity?

What reputational damage would be avoided?

What kind of natural disasters are likely and how fast will you recover?

Can the solution help avoid paying a ransomware ransom?

How will the solution ease compliance audit preparation and avoid fines?

INEFFECTIVE STRATEGY #2: INVOLVING TOO MANY SYSTEMS, SOLUTIONS AND PROCESSES

While downtime is blamed on many factors, there s one underlying obstacle to achieving reliable continuity: the complexity of most BDR solutions. Over the years, many teams have acquired a variety of point solutions that ultimately bog them down in a quagmire of arduous processes. By stitching together a Frankenstein s monster of solutions and vendors, the team finds themselves struggling with tools that don't talk to each other, support teams that dodge responsibility and time-consuming processes that prevent them from focusing on their core mission. These clumsy systems almost always mean delays in recovery and labor-intensive backups.

Complexity cannot coexist with fast and efficient recovery. Today's advanced BDR solutions that offer near-instant recovery work so well in part because they are simple. Features like one-click recovery and intuitive dashboards, where anyone can grasp the failover process without training, are key to banishing downtime. Automated testing, built-in compliance, easy throttle features and other offerings also simplify (or eliminate) tedious hours of labor.

Only that level of simplicity and efficiency will help them sidestep panic and frustration when downtime hits. By going to an all-in-one solution that offers easy backups, fast recovery and high availability, teams can get back to more purposeful work that supports the organization s goals.

64
SIXTY FOUR
64% of organizations use more than 3 different BDR solutions.

26
TWENTY SIX
26% use more than 5.

90
NINETY
90% want a unified dashboard.[2]

[2]Quorum State of Disaster Recovery Report, 2016

INEFFECTIVE STRATEGY #3: TREATING ALL DATA AND SYSTEMS AS EQUALS

Today s typical organization is an ecosystem of intertwined systems and applications. The massive amounts of structured and unstructured data floating through different departments and locked in different silos often makes it difficult, if not impossible, to understand where the most critical resources are and the best strategies to protect them. As a result, teams will allocate equal protective measures across the board, wasting firepower on unimportant resources while leaving other critical systems and data without a strong, secured recovery plan.

Most teams can de-fang downtime by keeping their email and transactional applications running while they fix whatever problem has taken them down. Analyze the differences in criticality between systems and data and you ll be able to allocate resources more strategically, saving budget while strengthening recovery.

To get a clear idea of which assets to prioritize, consider the following:

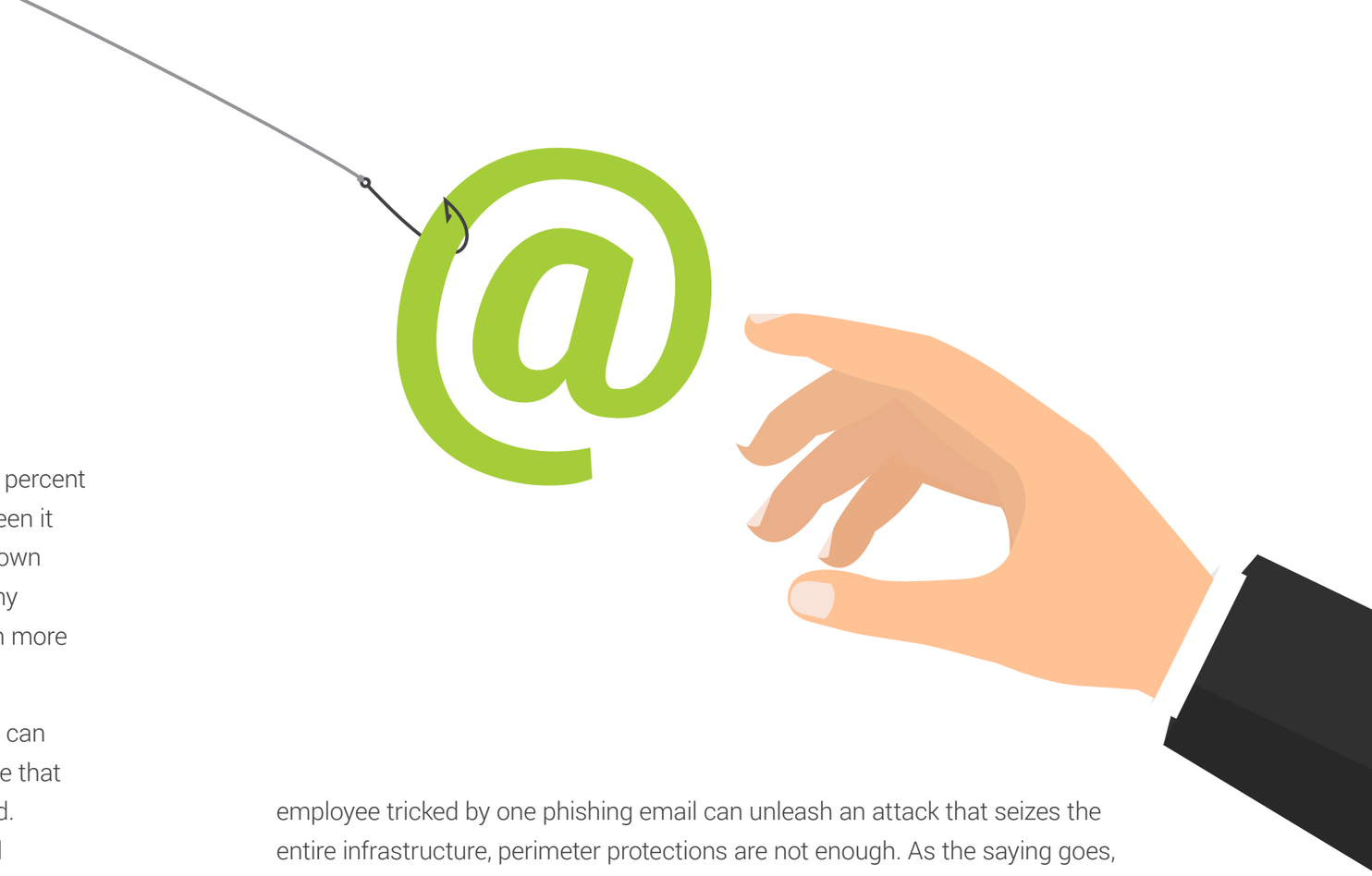
System and application integration. If you re like most organizations, you ve combined your applications in a value or supply chain. But often this means they re managed and monitored in silos, impacting visibility and making it harder to get the big picture necessary to intelligently steer the entirety of the infrastructure. If a system in one silo goes down, it might impact another system but without that oversight, you won t be able to anticipate the effect to your entire IT sphere.

RTO for specific applications. How fast do you need to recover? as a general question isn t useful; multiple systems will have varying levels of urgency. An application accepting resumes for Human Resources can afford to be offline for a few hours. The systems used to let customers load up shopping charts or access critical medical or financial data will need much faster recovery. The key to ranking individual RTOs: the cost impact analysis you did above in terms of lost business, reputational damage, wasted productivity and other factors.

Maintenance and service schedules. This factor often goes ignored: each application s maintenance schedule and service level requirement. Forget these and you may miss times when your mission-critical data isn t easily accessible. And if your solutions are going to require other point solutions as your needs get more complex or need major upgrades, you ll need to factor that into any planned changes to the infrastructure. Maintenance schedules may not seem too urgent when it comes to solving downtime, but they ll help you create an accurate data availability index and rectify any workflow gaps.

[2]Quorum State of Disaster Recovery Report, 2016

INEFFECTIVE STRATEGY #4: FOCUSING ON THE PERIMETER TO STOP RANSOMWARE



Ransomware attacks have been increasing exponentially in recent years a 300 percent rise in 2016[3], according to the Department of Justice. In recent months, we ve seen it break out of IT departments and become a staple of the evening news, taking down individuals and organizations large and small across the world. Even worse, many criminals are putting their ransom profits back into the business to develop even more advanced coding for more sophisticated attacks.

Ransomware is more than a financial hardship; it's a brand embarrassment that can permanently alienate customers and drive away employees. So it s not a surprise that many organizations have been desperate enough to pay the ransoms demanded. Organizations with business-critical systems such as companies in the financial services and healthcare industries are top targets. Yet paying ransoms often marks the company for a return visit, as the attackers know these teams don t have the BDR power to stop them.

Most business and IT leaders are taking steps to prevent becoming the next ransomware victim. However, their typical security controls focus on perimeter protections to stop the malware from penetrating their systems. Given that one employee tricked by one phishing email can unleash an attack that seizes the entire infrastructure, perimeter protections are not enough. As the saying goes, ransomware is not just a security issue, it s a recovery issue. Teams must dedicate their efforts where they will do some good: by creating fast and reliable recovery options.

Only rapid recovery will help organizations resurrect their systems without paying the ransom. Accurate backups that are immediately available are the only way to turn back the clock and save the organization and send the attackers packing.

[3]**Department of Justice,** How to Protect Your Networks From Ransomware

INEFFECTIVE STRATEGY #5: IGNORING THE POTENTIAL OF THE CLOUD

Despite the much-lauded advantages of the cloud, many organizations are still sticking with on premises backups as the entirety of their system. Rather than using cloud services to supplement or even replace traditional backup and recovery infrastructures, these teams often feel safer relying on a physical repository of backups, believing them safe from cyberattacks and other threats.

In reality, these teams make themselves vulnerable in several ways that almost guarantee long downtown windows. Corrupt or disintegrated tape backups, difficulty in accessing offsite datacenters, theft and natural disasters such as flood and fire can all leave an organization stranded when an outage hits.

Can on premises BDR still play a valuable role in modern recovery? Yes. But when it comes to speed, cost savings and performance, adding another layer of security in the form of cloud backups can be the most reliable way to reduce or eliminate downtime. Even when a hurricane or electrical fire takes down an offsite datacenter, or tape backups are found to be unusable, those cloud backups can provide a flawless replica of your environment available instantly.

Your team has several options when crafting a cloud-based BDR strategy. You can choose between data and workload hosting, hybrid cloud or Disaster Recovery as a Service (DRaaS); with a variety of configurations and options to suit your needs, you can leverage your existing infrastructure while still enjoying the rapid recovery, high, performance and cost savings of the cloud.

24

TWENTY FOUR

24% of respondents are using only on premise disaster recovery solutions as opposed to leveraging the cloud.[4]

[4]Quorum State of Disaster Recovery Report, 2016

ACHIEVING THE ULTIMATE UPTIME

Organizations that want to compete at the top of their field cannot afford downtime. To achieve consistently high uptime and performance, IT leaders must understand the factors that matter in recovery and data management and the factors that don t. Speed and simplicity, cloud-based redundancy and a tiered recovery strategy tied to economic impact are the keys to eliminating downtime and protecting organizations.

Yesterday s solutions can t solve tomorrow s threats. Instead of treating backup and disaster recovery with indifference, teams must prioritize partnering the right solutions with the right strategies for IT protection and business success.