MAINSTREAM TECHNOLOGIES

We create, manage, and secure technology

Tech Simplified

as IT should be

Our partners expect it.

Shouldn't you?

WINTER 2022

Inside

TOYING WITH DISASTER

Reduce the risk of catastrophic data loss with managed backup and disaster recovery services.

During the making of Pixar Studio's computer-animated classic Toy Story 2, a studio employee accidentally deleted about 90 percent of the film, roughly two years' worth of work. Worse, the company soon discovered that backups had failed. Catastrophe was averted only because a technical director who had been working from home while caring for her newborn child had everything backed up on her home computer. The finished film went on to become one of the most profitable animated films of all time, with global box-office receipts of more than a half-billion dollars.

"That story is legendary among data protection professionals because it demonstrates just how important it is to have effective backup and disaster recovery solutions in place," said Mark McClelland, Mainstream Technologies co-founder and vice president of IT. "But even though the consequences of data loss are well understood, you'd be surprised how many businesses don't make backup and recovery a priority."

Two recent studies illustrate the breadth of the problem. An IDC study finds that 60 percent of organizations across North America and Western Europe experienced unrecoverable data loss over the past 12 months, largely due to infrequent, inadequate or nonexistent backup routines. Meanwhile, a global survey from Dimensional Research finds that only about a quarter of companies have a documented disaster recovery plan that is regularly tested and updated.

Why would anyone risk catastrophic data loss? Many say it's because the whole backup and disaster recovery (BDR) process has become too difficult — and too unreliable.

DATA PROTECTION CHALLENGES

Backup processes become more complicated, time-consuming and expensive as more data is scat-

tered across multiple cloud platforms, branch offices and endpoint devices. In a survey of data storage professionals, 53 percent identified complexity of backup systems as their top challenge. More than 40 percent reported they must administer 10 or more devices for storage, backup and disaster recovery — each with separate processes and management systems.

Even those who do perform backups often experience data loss anyway. Nearly 60 percent of all backup jobs fail, according to a recent Vanson Bourne survey. Poor management and monitoring processes, missed alerts and configuration errors are among the leading contributors to backup failures.

Data protection is particularly challenging for small to midsize businesses (SMBs). With limited IT staff and budget constraints, BDR often gets prioritized out of the picture. Although they may understand the risk, SMBs often elect to focus their resources on other IT priorities.

THE MAINSTREAM SOLUTION

A comprehensive managed backup and disaster recovery solution such as Mainstream's GetITBack service is a cost-effective way to reduce the risk of catastrophic data loss while offloading management headaches. Mainstream has expertise in a variety of backup environments and can deliver high levels of stability and predictability.

"Data protection is a core component of our solutions portfolio," said McClelland. "With deep experience in the latest backup technologies, techniques and tools, we can ensure optimal data protection based on industry-accepted best practices. Our service reduces your risk profile while allowing you to optimize costs and offload staffing and management burdens."

One way Mainstream maximizes data protection is with a 3-2-1 backup strategy, which states that organizations should store three copies of their data on two different types of media, with one at an offsite location. Mainstream adds another layer of protection with an immutable backup option — a write-once, read-many backup that cannot be altered or deleted, even by an administrator. It ensures an untouched version of data is always recoverable and safe from any ransomware attack or system failure.

LAYERS OF PROTECTION

GetITBack offers options for additional protection. For example, customers can use Mainstream's SSAE 16 Type II data center in Little Rock and our other redundant failover sites to create the geographic separation necessary to safeguard data in the event of a disaster that incapacitates their main corporate site. Backup encryption creates another layer of protection in the event of data loss or theft. It's also a requirement for compliance with regulations such as PCI-DSS and HIPAA.

Mainstream also extends data protection across the customer's entire organization. Software agents installed on physical and virtual servers back up data to appliances deployed at the customer site. The appliances keep a copy of the backup images and also replicate them to an offsite location such as cloud storage or one of our data centers. The use of appliances speeds the recovery process by offloading the computing workload that would typically run on a local server.

Testing is one of the more critical — and overlooked — benefits of a managed BDR solution. Multiple studies find that fewer than half of organizations test their plans, increasing their risk of a recovery failure. With GetITBack, Mainstream conducts quarterly tests to verify that backups are working properly and that data, files, applications and other resources can be reliably accessed and restored.

"Data is perhaps the most valuable asset in the digital age, but few organizations have the skills and resources to maintain an effective data protection strategy," said McClelland. "A managed BDR service such as GetITBack reduces the risk of catastrophic data loss by simplifying the protection and recovery of data throughout the organization."

TECH SIMPLIFIED

Editorial Correspondence:
10221 E. 61st Street
Tulsa, OK 74133
Phone (800) 726-7667
Fax (918) 270-7134

Change of Address: Send corrected address label to the above address.

WHAT'S THE PLAN?

The differences between disaster recovery and business continuity plans, and why you need them both.

Every business needs a plan for responding to events that could cause prolonged unavailability of critical IT systems, services and applications. However, industry surveys consistently find that roughly half of all companies have no such plan in place.

Cost plays a role. Small businesses, in particular, are reluctant to tie up capital in processes and technologies they might never need. Another issue is the widespread misunderstanding of what processes and technologies constitute an effective business resilience plan.

"Most business owners recognize that data loss and downtime represent serious threats to their organizations, but they don't always understand all that's required to respond to those threats," said Mark McClelland, Mainstream Technologies co-founder and vice president of IT. "A lot of companies think having good data backup with offsite storage is sufficient. That's certainly an important component of business resilience, but it isn't nearly enough.

"In a worst-case scenario, what is your plan for finding new office space, new desks, new computers and new telephones? How will you maintain contact with your employees, customers and business partners? Ensuring data survivability alone will not keep a business going in the event of a catastrophic event."

WORKING TOGETHER

Every organization ought to have robust Disaster Recovery (DR) and Business Continuity (BC) plans that guide its response to business disruptions. Unfortunately, a lot of companies still think DR and BC are interchangeable labels for the same thing. While they are complementary processes, they serve markedly different purposes.

Disaster recovery is a tactical procedure focused on the recovery of technology assets such as systems, networks, applications and data. An effective DR plan includes data-retention policies that are compliant with the ISO 27000 series of international standards for information security management. These standards include, among other things, offsite data storage, data recovery metrics and controlling both electronic and physical network access in order to protect corporate assets.

DR is actually an important component of business continuity, but BC planning is a far more strategic process comprising a broad range of factors necessary to continue operations in the event of a business disruption. A BC plan addresses not only data safety but facilities management, human safety, risk management, personnel policies, intellectual property and internal communication procedures.

MORE THAN TECHNOLOGY

"Disaster recovery is viewed as principally an IT effort, but a business continuity plan provides a blueprint for

the entire organization," said McClelland. "It makes the connection between IT managers and business managers and between companies and their partners. It requires the cooperation of a company's management at all levels, as well as the involvement of key partners and suppliers."

An important element of a BC plan is a business impact analysis (BIA), which starts by listing all business functions, ranked in priority according to which must be back in operation first. The BIA should further identify and evaluate the operational and financial consequences of a disruption to each function. Among the factors to consider are lost or delayed sales, increased spending, regulatory fines, contractual penalties and reputation damage.

Once priorities are determined, recovery time objectives (RTO) and recovery point objectives (RPO) are established for each function. The RTO is the allowable amount of downtime before the function is brought back online, while the RPO is the allowable amount of data loss since the last backup.

OTHER CONSIDERATIONS

A plan must include an assessment of the threat landscape and the identification of strengths and weaknesses across the organization. In addition to technological considerations, the roles and responsibilities of key personnel before, during and after an incident should be clarified to ensure that the BC plan is properly executed.

A BC plan should also address supply chain risk and contingency management. Shipping delays, product shortages, manufacturing backlogs and other challenges during the pandemic continue to create limitations for companies in most industries. The plan should identify alternative sources for essential products and materials as well as additional transportation and shipping options.

"Having a solid plan in place is no guarantee it will work as expected," said McClelland. "That's why it's critical to test your DR and BC plans to verify everyone knows what to do. Managers and team members should review plans regularly and conduct periodic disaster simulations and tabletop exercises to ensure everyone understands their roles and responsibilities."

HOST with the MOST

Mainstream's hosted data center services provide secure, scalable and cost-efficient disaster recovery resources.

Disaster recovery strategies have traditionally involved failing over to offsite IT infrastructure where workloads can continue to run without interruption in the event of problems at the primary data center. However, that can be extremely expensive. By some accounts, building a data center with redundant infrastructure can cost up to $1,000 per square foot.

Organizations are increasingly choosing to conserve costs by using hosted data center solutions rather than building, expanding or modernizing their own infrastructure. In a recent Ayaka survey of 1,600 IT professionals, 51 percent of respondents said they plan to close all of their on-premises data centers over the next two years, and 27 percent said they plan to eliminate at least some of their facilities.

"The costs and challenges of maintaining on-premises data center infrastructure have become more than all but the largest enterprise organizations can adequately handle," said Mark McClelland, Mainstream Technologies co-founder and vice president of IT. "That's why more companies are exploring data center hosting solutions that allow easy offsite failover of IT operations without the costs of building a physical DR structure."

Mainstream Technologies supports the disaster recovery and business continuity requirements of our customers with several hosting options. We deliver colocation, managed colocation and virtual private server offerings through our state-of-the-art data center, providing the security and easy access of on-premises infrastructure and the strategic, operational and financial benefits of the cloud.

COLOCATION

Colocation, or colo, provides a number of cost and management benefits. In a colocation arrangement, customers rent space in our data center facility for their hardware. The advantage is that they can build servers to their specifications, with the CPUs, RAM and other components of their choice. Customers can replicate their production environment to support their disaster recovery operations.

Colocation data centers offer multiple connectivity options and redundant components such as operating systems, processors, disks, controllers, cooling systems, fans and more to ensure resilience and high availability. Colo facilities also contribute to improved regulatory compliance because they are required to implement a multitude of security and privacy measures to protect customer data.

Advanced physical security features such as video surveillance, outdoor lighting, fences and other barriers, locks, alarms and access controls provide an additional layer of protection. Most facilities also offer IT security services such as managed firewalls, advanced threat detection, intrusion prevention, vulnerability testing, encryption and compliance validation.

MANAGED COLOCATION

While colocation relieves customers of many operational burdens, they remain responsible for managing and maintaining servers, switches, routers, VPNs, firewalls and more. Managing and maintaining gear at a remote data center can be a significant burden for organizations with limited IT staff — particularly if the colo facility isn't within easy driving distance.

In a managed colo arrangement, the provider extends all the benefits of a traditional colocation arrangement by also taking on the bulk of administrative and management functions for a predictable monthly fee. Providers typically offer "remote hands" services that cover basic tasks such as rebooting a server, reconnecting cables or responding to alerts, as well as "smart hands" services for more complex tasks such as server provisioning or configuration changes. This is particularly valuable if a disaster prevents IT personnel from traveling to the colo facility.

VIRTUAL PRIVATE SERVERS

Mainstream's VPS hosting service uses virtualization technology to provide customers with dedicated resources on a server with multiple users. This approach relieves customers of the need to purchase and own servers. Instead, they simply pay a monthly subscription fee to access virtual server instances in our data center. It's the functional equivalent of a dedicated physical server, but with the cost benefits of a virtual machine.

VPS hosting is different from other types of shared hosting plans in which multiple customers share all the server resources, including bandwidth and storage. VPS hosting ensures each customer has access to an exclusive set of resources by creating partitions between multiple virtual servers. While all the virtual servers share a hypervisor and underlying hardware, each VPS runs its own operating system and software and reserves its own share of server resources such as memory and compute. It provides a cost-effective means of recovering virtualized services in the event of a primary site disruption.

"Some organizations still want the total control they can achieve with an on-premises data center, but the costs of building, expanding and managing these facilities is becoming an unnecessary expense for most," said McClelland**.** "Hosted data center solutions address these issues by providing the facilities, cooling, power, bandwidth, staffing and security and physical security."

>>> Physical Security

When considering hosted data centers, it is extremely important to evaluate how providers protect people, property and assets.Here is a checklist of basic physical security features that every facility should have:

> **Door security and alarms.** Every entrance or exit, including windows, should have industrial locks and sensors that trigger alarms. Important rooms inside the facility, such as server rooms and document storage rooms, should be similarly protected.

> **Access controls.** Keys, smart cards, badges, biometric scanners and other tools for validating a person's identity prevent unauthorized personnel from entering your building.

> **Video surveillance.** Modern video surveillance systems provide high-quality footage that can be remotely monitored and managed. Video cameras also serve as deterrents to both internal and external threats, so experts recommend leaving them visible.

> **Fire suppression.** Sprinkler systems are the most common fire suppression systems, but clean agent systems that use non-conductive, non-corrosive gases are even better for data centers because they leave no residue and won't damage sensitive equipment. Systems should be monitored at all times and serviced regularly.

> **Redundancy.** All electrical, mechanical and environmental systems must have built-in redundancy to ensure there is no single point of failure. The electrical system should be fully redundant with multiple distribution paths to IT equipment. Find out how many distribution units, backup systems, utility feeds and generators are in operation.

> **Personnel.** Many people just assume that a hosted data center will be staffed. Make sure you're not going with a so-called "dark site" that is not staffed.

Mainstream Technologies
3212 NW Avignon Way
Bentonville, AR 72712

tech simplified

MAKING LIVES BETTER THROUGH TECHNOLOGY

Just ask some of our partners

MAINSTREAM TECHNOLOGIES

Arkansas Secretary of State JOHN THURSTON

ANDREA LEA AUDITOR OF STATE

BALDWIN & SHELL CONSTRUCTION COMPANY Building Relationships

WINTHROP ROCKEFELLER INSTITUTE UNIVERSITY OF ARKANSAS SYSTEM

Goodwill Industries of Arkansas

LITTLE ROCK REGIONAL CHAMBER LOVE, LITTLE ROCK

PHILANDER SMITH COLLEGE

BELL company N. Little Rock | Conway

325 W. Capitol Ave., Ste. 200, Little Rock, AR 72201