arcserve®

The Current State of Data Protection in Midsize Organizations

introduction

In our "always on" business climate, safeguarding valuable data has never been more important. But, many data protection and availability plans were developed in an era where ransomware wasn't a key issue or the term, "big data" hadn't become commonplace.

Today, the IT teams that manage business-critical systems, applications and data have a new set of challenges to worry about: increasing data and system complexity, the explosion of ransomware/malware attacks, data loss and its resulting penalties, and identifying the right data protection and availability solution to mitigate these demands.

To better understand how IT strategies are evolving, Arcserve commissioned an independent survey of 283 IT service providers, resellers and consultants to uncover the key data protection trends and concerns of midsize organizations.

table of contents

Managing and protecting complex systems, applications and data

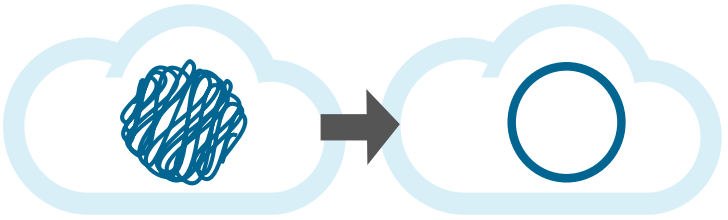
The data protection space is evolving with a myriad of new challenges, so it's not surprising that many midsize organizations are drowning under volumes of data and subsequently, the challenges of protecting it.

The reality is that more data has been created in the past two years than in the entire history of the human race.[1] This alone adds strain on IT teams like never before, but compound it with the complexity of managing varied systems, applications and data, and you have a real mess.

96%
RUN CRITICAL APPLICATIONS ON PHYSICAL SERVERS

Likewise, IT teams are rapidly changing and becoming smaller, yet are faced with the burden of managing complex data protection and availability solutions – many of which were chosen by specialists in the age of big IT teams with big budgets. And while these organizations have adopted virtualization or cloud-based solutions with the intent of simplification, their IT teams still need to support legacy systems.

According to our survey, the majority of IT service providers, resellers and consultants revealed that their midsize customers deploy hybrid cloud, virtual and physical infrastructures – with a whopping 96% indicating that these organizations run critical applications on physical servers. It's no wonder that nearly 65% of survey respondents said their customer's top data protection initiative is to simplify their backup IT infrastructure.



65% AIM TO SIMPLIFY THEIR BACKUP IT INFRASTRUCTURE

The key to managing data protection strategies across varied storage platforms is really about shifting the discussion from one where data loss is entirely an IT concern, to one in which data loss is a critical business concern. These conversations about business continuity – known as the planning, preparation and implementation of more resilient business systems – can enable the IT teams to unify and consolidate backup and recovery, whether on disk, tape, or in the cloud, and regardless of the data loss threat.

[1] http://www.forbes.com/sites/bernardmarr/2015/09/30/big-data-20-mind-boggling-facts-everyone-must-read/#7afaea6b6c1d

DID YOU KNOW?

You can reduce backup storage requirements by up to 95% with certain data deduplication techniques? Arcserve's global deduplication technology eliminates data redundancy across all of your storage systems, thereby significantly reducing your storage footprint and slashing infrastructure costs. And, since data is deduplicated before it's transferred to your target server, only changes are sent over the network, improving performance and reducing bandwidth usage.

"The ever-growing data presents a big challenge when it comes to backup. We estimated that in some months we were spending upwards of 20 hours fixing intermittent backup issues and a doubling of our backup footprint around every 10 months."

—Sean Dendle, Director of Cymax

The explosion of ransomware

As long as the Internet has existed, hackers have been behind the scenes creating viruses to infect devices or gain private user information.

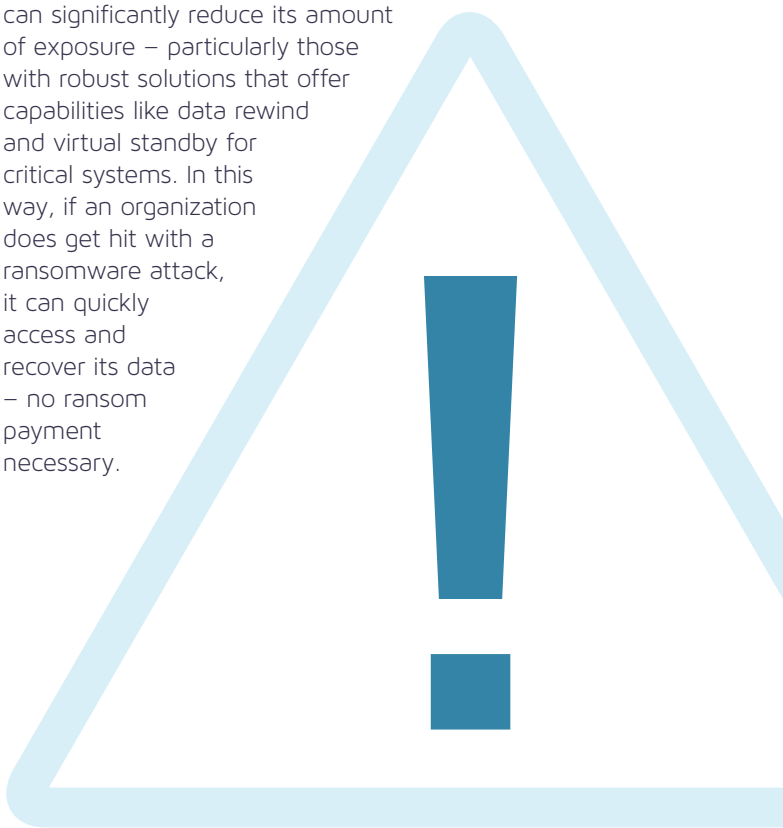
But over the past few years — largely driven by the advent of Bitcoin — a new data threat, commonly known as ransomware, has ascended to become one of the most problematic threats to organizations of all sizes.

This new breed of hackers, or cybercriminals, are making hundreds of thousands of dollars every month from holding business data hostage and demanding payment via Bitcoin, the cryptographic digital currency which offers a secure and often untraceable method of making and receiving payments.[2] Often, organizations will pay the "ransom" to get their data back but find it encrypted or unusable, leaving them paralyzed.

According to our survey, **nearly 60% of IT service providers, resellers and consultants say their midsize customers have been the victim of a ransomware attack in the past year** — and the frequency and cost continues to grow. Last year alone, the Internet Crime Complaint Center received 2,500 complaints of ransomware, costing U.S. victims $24 million.[3] And according to the Department of Justice, ransomware attacks have increased 300% so far in 2016.[4]

Because of the relatively simple nature of ransomware, which often tricks the user to click on a malicious link or attachment, the prevalence will continue to increase in the coming years. This means lost productivity and revenue, operational risk and inefficiency, and reputational damage. However, even knowing this, most organizations don't have a fallback plan and many resort to paying the ransom (which isn't recommended).

Today's organizations must not only have preventative measures in place, such as strong spam filters and user awareness training programs, but also a business continuity plan that includes a proven data protection and availability solution. With regular backups, an organization can significantly reduce its amount of exposure – particularly those with robust solutions that offer capabilities like data rewind and virtual standby for critical systems. In this way, if an organization does get hit with a ransomware attack, it can quickly access and recover its data – no ransom payment necessary.



[2] http://www.zdnet.com/article/how-bitcoin-helped-fuel-an-explosion-in-ransomware-attacks/
[3] http://finance.yahoo.com/news/victims-paid-more-24-million-222700088.html
[4] https://www.justice.gov/criminal-ccips/file/872771/download

Data loss and its resulting penalties

One might argue that an organization wouldn't function without access to its data, systems and applications. But not all data is created equal.

Thus, the need for differing service level requirements based on the criticality of specific applications. Internal marketing documents or photos from the last employee picnic can typically withstand several hours of downtime, while transactional or point-of-sale (POS) systems are often mission-critical and must be available in seconds.

Ultimately, it's a numbers game, and the ability to clearly identify and meet key data protection numbers can mean the next unplanned downtime event doesn't need to end in disaster. To achieve this, organizations need to answer the key question, "how much data can we afford to lose?" **IT service providers, resellers and consultants in our survey revealed that nearly all of their midsize customers have succumbed to data loss in the past year alone, with over half reporting it as a top IT concern.**

But it's not just transactional systems that need to be available. Organizations can easily overlook industry regulations, some of which they may or may not know exist. Currently, the U.S. has about 20 sector-specific national privacy or data security laws, with hundreds of others specific to each state and territory. Midsize businesses are subject to the same data availability and data protection requirements as large corporations for regulations such as HIPAA, Sarbanes Oxley and SEC Rule 17, but without the big budgets to meet these requirements. Unfortunately, consequences (i.e. monetary fines) can be substantial.

At the end of the day, an organization's ability to quickly recover business-critical data will be paramount to its future success. Whether caused by natural disaster or human error, downtime – particularly for midsize businesses that may not have vast resources at their disposal – can wreak havoc on your bottom line.

IS YOUR DATA AT RISK?

If you can check two or more of the following boxes, your organization may be vulnerable:

- ☐ Are your employees global – or located across multiple time zones?
- ☐ Does your organization rely on transactions through your website, or do you have a substantial e-commerce business?
- ☐ If a downtime event occurred, would your business face legal issues and fines pertaining to records management, HIPAA mandates, or other federal regulations?
- ☐ Would it take you more than a few minutes to restore access to mission-critical systems?
- ☐ Would multiple manual interventions be required to restore data during a downtime event?

The Real Cost of Downtime

Restoring data is more than just copying data back from the cloud, tape or a backup appliance; it also includes the time required to bring all of your users or customers back online. Planned or unplanned network outages can set off a chain of costs and consequences. These may be direct or indirect, tangible or intangible, short or long term, immediate or far-reaching.

According to the International Data Corporation,[5] 80% of small and midsize businesses have experienced downtime with associated costs ranging from $82,200 to $256,000 per event. Gartner estimates the hourly cost of network downtime for large corporations at $42,000, with a typical business experiencing an average of 87 hours of downtime a year, resulting in total losses exceeding $3.6 million.[6]

These figures emphasize that data availability can no longer be a "goal" of the IT organization, but a business challenge that must be realized.

[5] International Data Corporation: The Growth Opportunity for SMB Cloud and Hybrid Business Continuity
[6] http://www.zdnet.com/article/average-large-corporation-experiences-87-hours-of-network-downtime-a-year/

Data protection and availability solutions – which one is right for your business?

Though midsize organizations often have the same data protection requirements as large enterprises, they may not have the same large-scale budgets to ensure data availability for their critical systems and applications. What's more, many organizations have a tendency to deploy a variety of "passable" niche solutions to protect hybrid cloud, virtual and physical data. This layered approach of deploying siloed point products often creates significant challenges:

- Bloated investments of time and staff to manage complex data stores
- Cascading IT training expenses to develop highly-specialized skills
- Swelling infrastructure costs for multiple data protection solution purchases and maintenance renewal fees
- Increasing data loss risks as infrastructure complexity grows
- Expanding likelihood of compatibility issues

With modern technology, **midsize organizations should never feel forced to implement "one-size-fits-most" data protection solutions, which are often confusing, cost-prohibitive and about as unnecessary as a carwash during a thunderstorm.** Instead, businesses can save substantial time and money by partnering with a provider that offers:

- Seamless data protection and availability across cloud, virtual and physical environments without burdensome forklift upgrades
- Robust solutions to meet a wide range of RPOs/RTOs – enabling IT staffs to cost-effectively apply the right level of protection to diverse systems, applications and data
- Quick time-to-value with easy deployment and management – eliminating the need for extensive and costly professional services
- Comprehensive capabilities that combine high-performance technology, often found in multiple point products, into a single solution suite
- Choice in how IT leaders protect data with recovery and availability to and from any target, whether deployed via software, appliances or from a cloud (or a combination thereof)

WORKSHEET

Three Quick Steps to Determine Your Best-Fit Data Protection Solution

If you're considering a new data protection and availability solution, use the following three steps to help determine the best fit to meet your unique business and IT needs.

STEP 1

Take some time to assess your current and future data availability needs for every system and application, including storage size and infrastructure requirements. Ask yourself:

- ☐ What is your preferred method to protect from data loss?
  (e.g. disk to disk, disk to cloud, disk to disk to cloud, tape drive, disk to disk to tape or optical disk drive)
- ☐ Are there specific data availability or records management requirements for my industry or organization?
  (e.g. HIPAA regulations and corporate mandates)
- ☐ How quickly do I need to access specific systems, such as internal SharePoint sites, transactional applications, and customer databases?
- ☐ What systems and applications are interdependent? How would unplanned downtime for one system affect the others?
- ☐ What are my maintenance schedules and service level requirements for each system and application?

STEP 2

Not all data protection and availability solutions provide the same capabilities, particularly across cloud, virtual and physical infrastructures. Assess your specific concerns to determine what capabilities your data protection solution should deliver.

- ☐ Reducing the operational costs of backup and recovery
- ☐ Stretched IT resources or staff without specialized skills to deploy and manage your data protection solution(s)
- ☐ Growth or complexity of managing structured and unstructured data
- ☐ Control over application-specific RTOs/RPOs
- ☐ Inability to scale the level of data protection as business/IT needs change *(e.g. add on public/private cloud support, protect or expand protection for virtual environments, leverage high availability, etc.)*
- ☐ Expanding storage footprint and the associated high costs
- ☐ Lack of reporting visibility/transparency with internal stakeholders across the organization
- ☐ Burdensome backup times and bandwidth requirements
- ☐ Improving the speed of recovery
- ☐ Implementing a cloud platform for backup or disaster recovery
- ☐ Cost-effectively protecting remote locations *(e.g. data center, office branch, home office or cloud target)*

STEP 3

Understand where data protection solutions often fall short in customer expectations or needs. Before deciding on a solution, evaluate if it falls short in the following scenarios:

- ☐ Enables backup data from a single site, but doesn't always provide built-in replication to another disaster recovery site
- ☐ Protects physical systems well, but not virtual environments – or vice versa
- ☐ Doesn't allow backup of data to a public or private cloud
- ☐ Isn't agnostic to current systems or applications (introduces compatibility challenges)
- ☐ Can't be deployed in various modalities/give you the choice of software, appliances and cloud
- ☐ Doesn't enable flexible recovery specific to varied data, systems and applications *(e.g. restores in minutes – not seconds)*
- ☐ High-performance capabilities aren't built-in to the solution – or offered at all *(e.g. global data deduplication, automated disaster recovery testing, instant bare metal restore/VM recovery and virtual standby, enterprise storage array snapshot support, advanced protection for Windows and Linux systems, etc.)*
- ☐ Doesn't allow easy migration of servers and data from P2P, P2V, V2V, and V2P

Arcserve® Unified Data Protection (UDP) solution suite — enterprise power, small team simplicity

As organizations continue to face evolving data availability needs threats, it will become more critical than ever to find a solution that combines enterprise-grade capabilities without the complexity and cost associated with enterprise solutions. That's where the power of Arcserve's Unified Data Protection (UDP) solution suite comes in.

Through its complete range of capabilities, only Arcserve UDP allows organizations to cost-effectively apply the right level of data protection to unique systems – eliminating the need to layer on complex point solutions as business needs change. With one elegantly simple user console, organizations holistically configure and manage all aspects of their data protection strategy, from long-term storage to instant recovery, with complete control and visibility across all systems, applications and data.

We've invested over five-million development hours into our award-winning solution suite to guarantee data availability across cloud, virtual and physical infrastructures – with the flexibility to be deployed as software, appliances or in the cloud.

Try it for yourself with a **30-day free trial**, see how organizations are **successfully using Arcserve UDP**, or learn more about Arcserve by visiting **www.arcserve.com**.

Looking for some additional resources?

Data and Infrastructure Resource Estimator

Get an individualized resource assessment that accounts for your future data growth and the expense of added storage, complete with projected costs and savings for you to share with your team.

Data Deduplication Calculator

Exponential data growth and its associated storage costs can be easily overlooked or considered a routine factor in today's business climate. See how Arcserve's unique deduplication technologies can save your organization up to 95% in data storage requirements – and the associated high storage costs.