HOW FOCUSING ON DATA STORAGE CHALLENGES HELPS IT LEADERS ACHIEVE GREATER CYBER RESILIENCE

Establishing cyber resilience continues to grow in difficulty thanks to three main factors: 1) a rapid and continuous increase in data generation, 2) an increase in IT complexity thanks to factors like remote work, and 3) a continuously growing volume and frequency of cyberattacks. Trying to simplify IT and get a better understanding of your data and how to protect it is an uphill battle for IT leaders.

On top of this, additional pressure to achieve cyber resilience is being fueled by data privacy regulations that are starting to come out of grace periods—doling out hefty fines. There are many companies that have already been fined significant amounts of money. IT leaders are under a great deal of pressure and need to get a handle on the challenges of cyber resilience so they can start making changes that help them better prepare for cyberthreats while lowering risk of non-compliance.

Cyber resilience initiatives cover a broad range of areas from employee happiness to DevOps. It has become increasingly difficult for IT leaders to prioritize and find the best places to focus their limited resources.

When looking across this range, the area with the biggest potential for improvement is in data storage. This is where IT leaders can focus to achieve a real impact on cyber protection.

A 2020 ESG survey found that more than half of organizations have greater than 250TB of data, and 29 percent have more than 500TB of data. Data volume can be overwhelming, but the bigger

struggle is the fact that this data resides across many different storage solutions from the mainframe to SaaS providers. And a different approach is needed for each storage type. Data storage is where IT leaders need to focus for the biggest impact.

This article will cover the challenges faced with each type of data storage as well as tips on how to overcome these challenges. Additionally, we will discuss the positive impact on the business in making changes in data storage.

Focusing on data storage will positively impact cyber resilience

Breaking down this initiative into phases will help IT leaders to manage continued progress and show results to executives. More importantly, after each project phase you will be able to deliver compelling results back to the business.

The four phases of building cyber resilience in data storage:

Phase 1

Project: Gain control over the security and backup issues with various data storage solutions and minimize where possible the storage types used.

Business outcomes: Improved recoverability with more control of backups from SaaS providers. Lower storage costs from consolidation of data storage solutions.

Phase 2

Project: Discover, identify, and classify structured and unstructured data in order to move it to the correct storage solution.

Business outcomes: Proof of lower risk of data privacy non-compliance. Proof of lower risk of data theft. Lower storage costs from eliminating or archiving unneeded data.

Phase 3

Project: Put the appropriate security in place to protect your data backups from cyber threats.

Business outcomes: Evidence of improved security with a list of multiple measures that can be explained to executives. Proof of compliance with security measures required for data privacy.

Phase 4

Project: Reevaluate and improve your disaster recovery capabilities, ensuring they meet business needs in all scenarios.

Business outcomes: Evidence of disaster recovery testing results for various scenarios meeting business objectives. Regular reporting showing continued improvement of recovery objectives.

Working through these four phases will yield positive results for cyber resilience as well as cost avoidance, ranging from storage costs to data privacy fines. Each phase provides clear evidence for business executives to prove the value of their efforts. In a time when cyber resilience initiatives are broad and the IT environment complex, a strong focus on data storage will pay real dividends for IT leaders.

Gaining visibility and understanding your data

The most common, fundamental challenge that IT leaders face in cyber resilience initiatives is gaining visibility and understanding of their unstructured data—whether stored on-premises or by cloud solution providers. Most companies have suffered from data sprawl combined with a lack of labeling and categorization standards for data stored on individual hard drives or cloud storage. Mergers and acquisitions, structural changes, and lift and shift migrations have only added to this problem.

Gaining visibility into your data in order to understand it is critical to lowering risk of exposure to breach or to violating data privacy regulations. Both scenarios are painful and costly. Additionally, understanding your data is a key step in helping you to eliminate unneeded data—thereby reducing the amount of data you need to backup.

A great step IT leaders can take here is to invest in an intelligent data management solution. Select a solution that utilizes artificial intelligence to identify unstructured content. Specifically, select one that is pre-trained to recognize things like resumes and invoices that may have personal information in them. These tools can also automate the classification and labeling of this data so you can make better decisions on where the data should be stored, who should have access to it, what level of protection is needed, and what backup strategy to implement.

Strategies vary by storage type

Most large organizations have a long list of data storage types including on-premises servers and mainframes, cloud storage, and various SaaS providers. This poses a challenge to IT leaders looking to ensure data protection and appropriate backup solutions across the various technologies and vendors.

Here are a few considerations that IT leaders need to be aware of for each storage type.

Cloud storage

Many companies have adopted public cloud storage for some of their data, resulting in large hybrid cloud infrastructures. As IT leaders work toward cyber resilience this often requires increasing storage capacity to accommodate rigorous backup needs.

To avoid additional costs, IT leaders should consider adopting software-defined storage solutions that can help them better manage their hybrid environment while maximizing their storage scale. This results in lowered storage costs as well as better performance in recovery. In fact, the case for software-defined storage solutions is so compelling that Gartner predicts that by 2024, 50 percent of global storage capacity will be deployed as software-defined storage.

SaaS

With so much data being generated and stored by third-party SaaS providers, IT leaders need to ensure they have a handle on SaaS backups. Unfortunately, there are no industry standards and backup scenarios for SaaS applications are rare. Yet there are many disaster scenarios where data loss can happen.

IT leaders need to assess the data protection and recovery processes before deploying new SaaS

applications. Contractually, it should be clear how data is backed up and accessed—both in case of a disaster and in ending the subscription. Ensuring alignment on recovery objectives is just as important as SLAs for uptime. Consider also deploying a backup solution that can support multiple SaaS applications, so you improve your recoverability while keeping complexity at a minimum.

On-premises & mainframe

While working on cyber resilience, IT leaders are finding that new advances in cloud storage and data protection management are providing opportunities to lower costs while maintaining, or even improving, cyber resilience. On-premises, tape-related backups are often complex, slow, and costly to maintain.

Moving mainframe backups to secure cloud data management and storage can significantly reduce storage costs, simplify operations, reduce backup times, and improve recoverability.

Data Recovery is a critical piece of the process

Once you've got your data backups protected, you still need to think about data recovery. IT leaders working on cyber resilience will likely find value in reevaluating their disaster recovery posture.

Key areas of disaster recovery evaluation are:

- Getting a clear understanding of business expectations on recovery and ensuring that recovery point and recovery time objectives can be met for each data storage solution.
- Considering the differences between various disasters such as data theft versus ransomware versus an outage and putting unique recovery plans in place for each. Be sure to consider recovery from different locations in this analysis.
- Planning for recovery performance by looking at ways to orchestrate the recovery process and make it faster. Figuring out the restore order for applications and databases is a necessary aspect of setting and meeting business objectives. Adding appliances to backup clusters can also increase compute without increasing capacity.
- Making maintenance and testing of disaster recovery a resourced part of operations where the team is not just testing for pass/fail, but looking for ways to continue to improve. Additionally, processes are needed to ensure backup and recovery systems are up to date on configurations and patching.

Backups alone are NOT a foolproof strategy

Once you understand your data and have made appropriate decisions in how to store it, you also have to determine how to appropriately back up critical data. Careful attention also needs to be placed on protecting the backups and ensuring they are accessible should recovery be needed.

Cyberattackers have turned the security backup trend into a new opportunity to exploit. More sophisticated attacks are now targeting backup data—to steal this data, wipe it, and/or to use it as a "roadmap" for the critical data in your system that they need to lock down for a ransomware attack. Combined with the steady increase in volume and frequency of attacks, this is a critical area for IT leaders to address.

This means cyber resilience requires increased focus on the protection of where data backups are stored and having more copies of those backups made and stored in different systems.

To meet these backup challenges IT leaders should focus on:

- Eliminating network sharing protocols when implementing storage as this is an area of weakness that attackers gain use to gain entry. Instead use secure object storage protocols or secure data movement APIs that utilize encryption in transit.
- Improving administrative permissioning by using multifactor authentication, separating administrative roles and creating multiperson authorization workflows.
- Implementing immutable file storage so that backup data can only be deleted in special circumstances, but not by a malicious actor.
- Ensuring multiple copies of backup data are made and stored at a disaster recovery site or within a cloud provider's infrastructure. Combine your copy strategy with immutable data storage and restrictive admin controls for best results.