



Quantum®

THE IT MANAGER'S GUIDEBOOK

ESSENTIAL STRATEGIES FOR
DATA PROTECTION AND BUSINESS
CONTINUITY IN TIMES OF CRISIS





TABLE OF CONTENTS

1. The Role of Business Continuance/DR
2. Preparedness
3. Security
 - a. Ransomware
 - b. Encryption
 - c. Setting Up a Remote Workforce with VDI (Virtual Desktop Infrastructure)
4. Data Protection
 - a. Backup Storage 101
 - b. Five Essential Backup Strategies
5. The Right Mix of Data Protection Technology
 - a. Tiered Storage for Your BC/DR Strategy
6. Cloud & Object Storage
 - a. Public Cloud
 - b. Hybrid Cloud
 - c. Object Storage
 - d. Enterprise Applications in the Cloud
7. What's Next? Justifying to Your CTO/CFO



It is 2020, and with the recent crisis the world has gone through, many IT organizations are on edge with new challenges about how to react to this new kind of threat, a nearly 100% remote workforce. It also has pushed many enterprises to focus more energy on planning for 'business continuity' and 'disaster recovery.' If we zoom in a little more for clarity, this is about security and data protection strategies when natural or man-made catastrophic events occur. It's about ensuring that all systems are "go" and by extension end points, as IT departments across many verticals and industries are called to respond with agility and swiftness during such crisis.

In this handbook, we will explore the main topics in the minds of IT professionals regarding business continuance and disaster recovery, and cover methods and strategies for developing a solid IT infrastructure that enables a resilient and effective plan before, during, and after a crisis.



PREPAREDNESS

A Word on Being Prepared

Protecting and storing data within the enterprise continues to get more complex as businesses manage exponential data growth across multiple platforms and environments—physical (on-prem), virtual, or cloud. Unstructured data sets in their various forms are growing by leaps and bounds and they are estimated to reach 1.1 YB by 2023 according to IDC's Global DataSphere Report. That is about 1,133 exabytes of capacity that will be shipped—all driven by unstructured data types, such as images, emails, surveillance, sensor logs, and video, to name a few.

To make matters worse, enterprise IT budgets are not growing nearly as fast as these unprecedented data storage requirements. In many cases, budgets are maintaining status quo, placing an emphasis on cost and operational efficiency. Then there is the data privacy and security issue. In this age of cloud computing, rampant cyber attacks, and regulatory pressures, businesses face a delicate balancing act.

The Road to a Solid Business IT Strategy

To effectively protect data across multiple sites and recover data quickly and efficiently in the event of a security incident, preparation and a solid

understanding of the organization's SLAs is the beginning of the road to a solid business IT strategy. Additionally, IT professionals must defend against ransomware and other cyber attacks, all while ensuring compliance with regulations such as GDPR.

Planning for a Remote Workforce

Maybe your IT organization is like Quantum's in that you have good planning in place to confront any conceivable storm and be prepared to weather it as best you can. *Having an established business strategy that allows your employees to work remotely as part of your normal business operations will be key in our new normal.* If you did not have a head start in the COVID-19 crisis of 2020, it's understandable, but there is no need to be in a reactive mode the next time. While nobody was ready for such a crisis, nonetheless, preparedness is key. To deploy a remote workforce that is cost effective, secure, reliable, and resilient takes time to develop and roll out as you prioritize hardware or software requirements within your infrastructure.

Let's explore these important topics that can help you not only survive the next crisis but help execute a planned strategy for a successful transition and ensure business continuity and disaster recovery for your enterprise.



SECURITY

Security is going to be a key consideration when deciding how and what platforms will be used to store your data. It is a comprehensive approach that will require multiple departments, as well as security professionals. Take the reasonable steps to educate yourself and your users, especially when you have a remote workforce. Identify where vulnerabilities might exist. Obviously, reputable cybersecurity software is recommended. Keep in mind that the last thing you want is for your data to be breached and ransomed.

Organizations need to have processes and policies in place on how to handle the security and availability of an organization's applications and data before allowing users to work remotely. Trying to create them on the fly (in crisis mode) will lead to increased risk and exposure. Here are six policies that should be addressed:

1. Avoid public WiFi.
2. VPN applications must be used (situational).
3. Endpoints should be encrypted and application traffic should be encrypted.
4. Implement multi-factor authentication.
5. Install/update antivirus software and well-defined network security policies.
6. Conditional access and compliance policies should be in place.

Regarding network security policies, consider using a cloud-native endpoint protection platform, including next-gen antivirus and endpoint detection and response (EDR), managed threat hunting, and threat intelligence automation. For example, the CrowdStrike Falcon Endpoint Protection Enterprise or Microsoft Defender Advanced Threat Protection.

Ensuring a solid business continuity plan is essential in helping you identify gaps and weaknesses. Adding a nearly 100% remote workforce to the fold and protecting those endpoints are now a critical component to any BC and DR plan.



Ransomware

Ransomware, due to the patience and tenacity of the criminals behind it, can sit and pause for any length of time, inspecting your network from a distance until they discover a way to bypass your security. This is not to say that cybersecurity software in the market today are not amazing solutions, but we know that cyber criminals are tenaciously patient and very hungry to be rewarded.

According to IDC research, 93% of organizations have been attacked within the past three years. This means that for most every organization, it's not a matter of if, but when. It is time to tighten up the integration of data protection, disaster recovery, and data security operations within the cybersecurity strategy and **think about backups as part of your cybersecurity approach**. Threats from ransomware and other malware are prevalent and there are plenty more threats engineered with AI capabilities to infiltrate your data center. Whatever cybersecurity software or backup method you choose (flash, SSDs, HDD, tape), or environment (physical, virtual, multi-cloud), the goal is to integrate what used to be silos and build a resilient IT operation.

The Latest Sophisticated Ransomware Threat

One note on the latest threat. Among the many strains of ransomware out there, there is one called REvil. REvil ransomware is a data-locking virus that was first spotted back in April 2019 by security researchers from Cisco Talos. Otherwise known as Sodinokibi/Sodin, the threat started off by exploiting zero-day vulnerability CVE-2019-2725. It allows attackers to remotely connect to the host machine with the HTTP access to Oracle's WebLogic server and inject the malware manually. As far as we know, there are no decryption tools available for this sophisticated threat, so you must have alternative methods to recover your data.

Whatever cybersecurity software or backup method you choose (flash, SSDs, HDD, tape), or environment (physical, virtual, multi-cloud), the goal is to integrate what used to be silos and build a resilient IT operation.



Encryption

You have heard the saying, “Safety first.” In the digital era, this statement has never been more important than today. It begins with a secured foundation at the server level (normally at the core). If your foundation is weak, the rest of your endpoints will probably resemble the same weak structure.

In-transit web data should always be sent via https. Also look at the various encryption models: client-side, server-side with service-managed keys, server-side with customer-managed keys. Also consider using a Key Vault to securely store keys. Do not take shortcuts. The following are ways to achieve a stronger security foundation:

Client-Side Encryption. Client-side encryption is performed outside of Azure. It includes:

- Data encrypted by an application that is running in the customer’s data center or by a service application.
- Data that is already encrypted when it is received by Azure.

With client-side encryption, cloud service providers do not have access to the encryption keys and cannot decrypt this data. You maintain complete control of the keys.

Server-Side Encryption. The three server-side encryption models offer different key management characteristics, which you can choose according to your requirements:

- **Service-managed keys:** Provides a combination of control and convenience with low overhead.
- **Customer-managed keys:** Gives you control over the keys, including Bring Your Own Keys (BYOK) support, or allows you to generate new ones.
- **Service-managed keys in customer-controlled hardware:** Enables you to manage keys in your proprietary repository, outside of Microsoft control. This characteristic is called Host Your Own Key (HYOK). However, configuration is complex, and most Azure services do not support this model.

Data should also be encrypted at rest. This includes data on server file systems and databases, but it also includes data on client endpoints. Most modern operating systems have disk encryption built in. For Windows 10 there is Windows BitLocker. For MacOS there is FileVault. To make administration easier, there are lots of products that allow you to centrally manage these endpoint encryption solutions.

Setting Up a Remote Workforce with VDI

Virtual data infrastructure is a very cost-effective solution that helps keep the data centralized and off endpoints, which are more susceptible to data loss.

It seems like security and remote workforce go hand-in-hand because of all the vulnerabilities associated with the most prevalent attacks on workers are outside the protected network of their enterprise. The scams run the gamut. As the threat to businesses continues, a large majority of organizations have turned to VDI to rapidly deploy virtual desktop infrastructures and release a mobile workforce that can be as productive as if they were in the office.

Virtual desktop infrastructure (VDI) is defined as the hosting of desktop environments on a central server. In other words, it's like having a structured office available on-demand

allowing you the ability to access virtual data and applications and you are really just shifting the compute cost from the endpoint to the data center (if on premise) or the cloud. Virtual data infrastructure is a very cost-effective solution that helps keep the data centralized and off endpoints, which are more susceptible to data loss.

Key advantages for deploying VDI for your remote workforce include:

- Break/fix becomes a lot easier because you can quickly “spin up” a new desktop for a user if their current desktop becomes corrupt.
- It makes things like patch management and OS updates easier since it is all centrally managed, which effectively lowers administrative overhead by adding additional compute resources easily without a full-blown fleet refresh.

DATA PROTECTION

Backup Storage 101

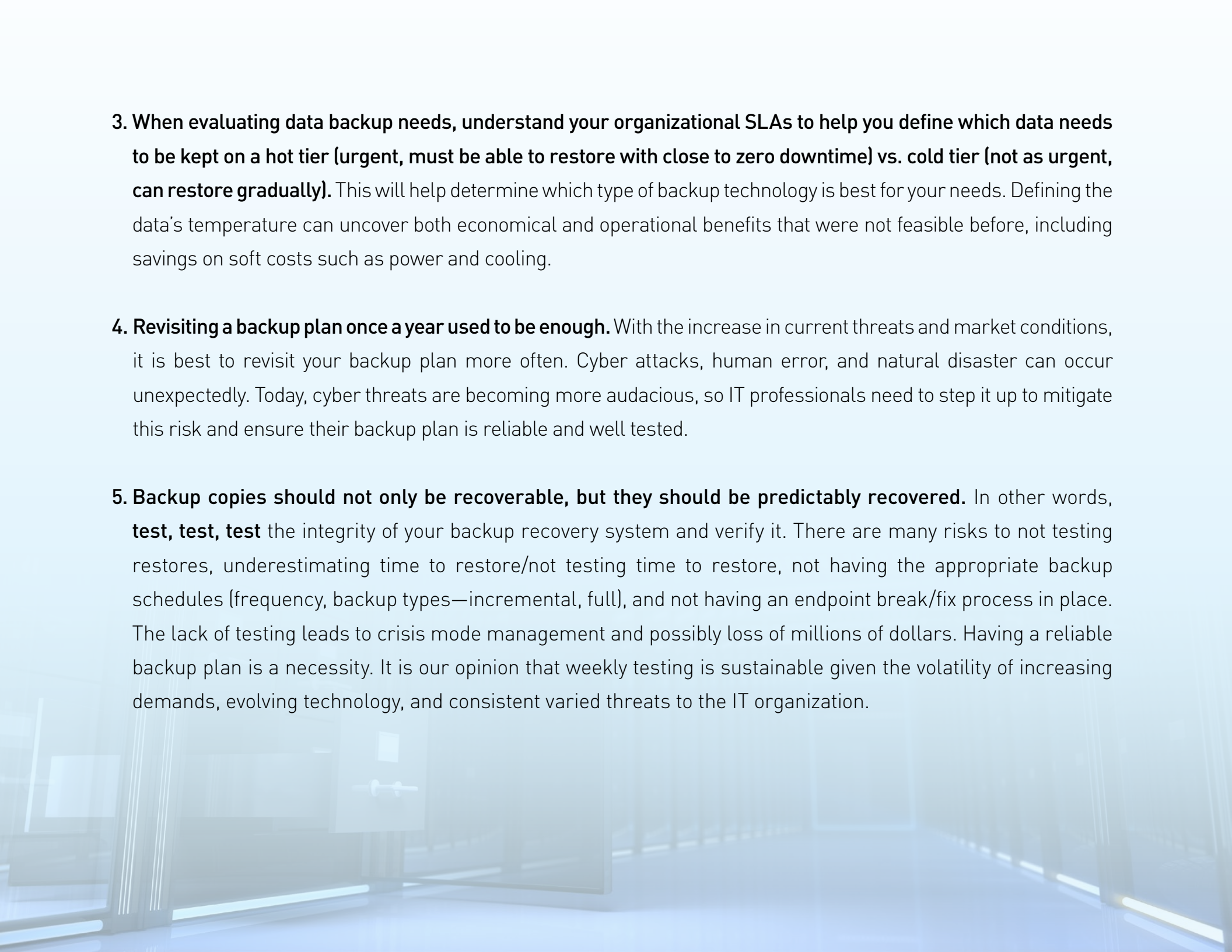
A little reminder can go a long way. It has never been more important to back up data regularly. COVID-19 was not a threat that was on anyone's radar and unbeknownst to it, many organizations were caught off-guard. This type of threat is on top of every other cyber threat, including ransomware, which is getting more sophisticated. We need to adapt and build IT environments to expect and withstand any type of attack.

With a remote workforce, endpoints will generate a lot of data and more IP will be leaving your premises. Intellectual property (IP), financial data, and personnel data are important data sets to be secured. What do you do? Going back to the basics is a good starting point. In the context of implementing security and protecting your data for continued operations in the midst of a crisis with nearly 100% remote workforce, *IT organizations are adjusting rapidly and quickly evolving to a new normal that may perhaps be the way of the future. It will help to remember that criminals are no longer using mass campaigns; instead, they are going for remote access where remote desktop protocol was the most used entry vector.*

Five Essential Backup Strategies

In the IT organization post COVID-19, building, securing, and protecting your data, your remote workforce, and your network are now high priorities, while upgrading to the latest AI or data management software is not as important as it once was. Best practices around data storage have not changed so much, but our reliance on software to be fully protected from different type of attacks has. Enterprises are realizing the importance of a solid backup strategy to protect data that includes an offline copy. It is essential to add an extra '1' onto the traditional 3-2-1 best practice rule for maximum data protection. There is now a need for a **3-2-1-1 approach**, where one copy of the data is stored offline as well as offsite. This protects against ransomware attacks by creating an 'air-gap' between the data and the network, thereby keeping it out of reach of hackers. Here are successful tips to add to your backup methodology:

- 1. Backups should be done daily.** If you suffer corruption, a breach, or complete data loss, how useful is a restore of incomplete data? Sure, you will have a starting point. But if crucial data is not backed up regularly, your restored data will be missing critical activity that took place since it was last backed up. This can cost countless dollars to repopulate, not to mention human resources that could be spent on critical data and applications vs. backups.
- 2. The 3-2-1-1 Rule – a rule proven true time and time again: Keep 3 copies of your data, using 2 different storage media types (object, flash, HDD, SSD, tape), 1 offsite (physically separate from the building such as DR site), and 1 offline (completely disconnected from your network).** Keeping a clearly defined data copy offline and air-gapped to protect against malware attack will enable you to retrieve that data and get back up to speed faster and back to business sooner in the case where your network-connected copies are compromised.

- 
- 3. When evaluating data backup needs, understand your organizational SLAs to help you define which data needs to be kept on a hot tier (urgent, must be able to restore with close to zero downtime) vs. cold tier (not as urgent, can restore gradually).** This will help determine which type of backup technology is best for your needs. Defining the data's temperature can uncover both economical and operational benefits that were not feasible before, including savings on soft costs such as power and cooling.
 - 4. Revisiting a backup plan once a year used to be enough.** With the increase in current threats and market conditions, it is best to revisit your backup plan more often. Cyber attacks, human error, and natural disaster can occur unexpectedly. Today, cyber threats are becoming more audacious, so IT professionals need to step it up to mitigate this risk and ensure their backup plan is reliable and well tested.
 - 5. Backup copies should not only be recoverable, but they should be predictably recovered.** In other words, **test, test, test** the integrity of your backup recovery system and verify it. There are many risks to not testing restores, underestimating time to restore/not testing time to restore, not having the appropriate backup schedules (frequency, backup types—incremental, full), and not having an endpoint break/fix process in place. The lack of testing leads to crisis mode management and possibly loss of millions of dollars. Having a reliable backup plan is a necessity. It is our opinion that weekly testing is sustainable given the volatility of increasing demands, evolving technology, and consistent varied threats to the IT organization.

THE RIGHT MIX OF DATA PROTECTION TECHNOLOGY

Let us start by asking the right questions.

1. Is your organization prepared to weather a cyber attack?
2. Is your network not only protected but resilient and able to predictably recover stolen, encrypted, or lost data?
3. What are the RPO/RTOs that need to be met, and can they be met with your current data protection technology?
4. If your network backup copies are compromised, do you have a copy offline and air-gapped?

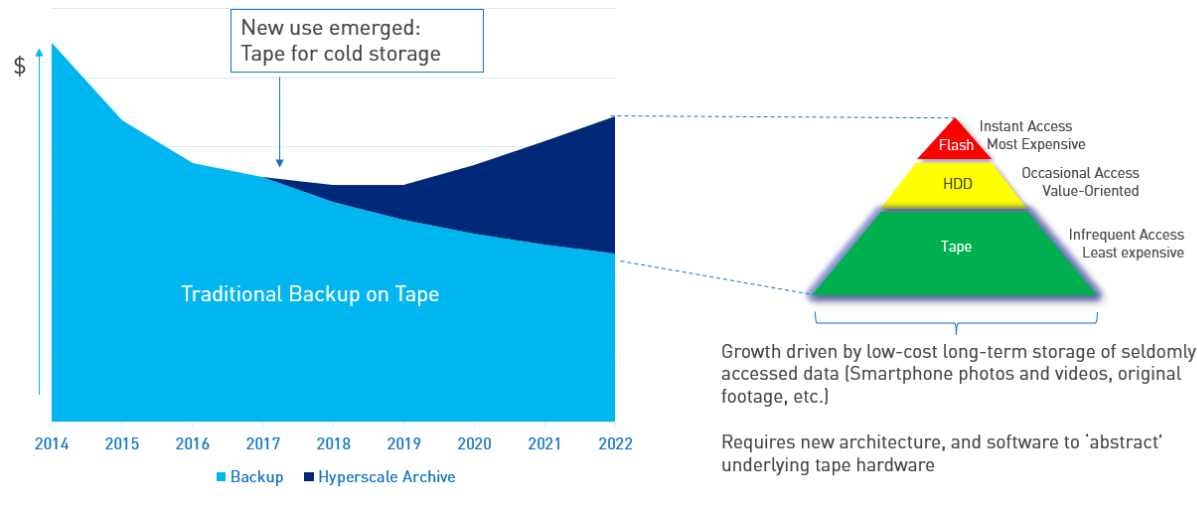
These and many more questions need to be asked to ensure that whatever data protection solution you choose, test your Business Continuity (BC) and Disaster Recovery (DR) to understand efficiency, resiliency, and predictability so you have the peace of mind that your data is protected.

Deploying the 3-2-1-1 Rule

The experts highly recommended that you apply the time-tested best practice rule of 3-2-1-1 to be safe. Have both disk and tape to ensure a reliable copy is available when you need it—whether you use cloud or hardware on prem, be it flash for hot data that requires fast processing to cold storage technologies for long-term retention, which is still the most cost-effective way to tier your data as it shifts in value. Object storage is not too far behind it in terms of cost when you leverage this technology in a multiple-copy scenario.

Tiered Storage for Your BC/DR Strategy

Shifting our focus to the topic of tiered storage is a good way to lead into the next, but not least important, subject on cloud and the efficient way to leverage new technologies. Traditionally, we thought about our storage in silos, on-prem appliances, and that method served us well for many decades. Technology advances, however, and the needs and demands of IT are increasingly more onerous simply because of what you are asked to do. To leverage the cost efficiencies of storage technologies that can be easily activated to implement in your BC/DR strategy, let us discuss the technologies available to do just that where price, performance, capacity, and function come into play.



Flash

The net result of using flash is screaming-fast performance. Using technology like NVMe will certainly allow you to process your content/data rapidly, but it does come at a cost. However, our data-driven world demands that organizations keep an agile always-on IT organization. Flash enables core cutting-edge applications to process content faster by accelerating all aspects of the workflow, providing ultra-fast reads and writes. Think of movie studios, research institutions, and government agencies that require performance out of their storage infrastructure. Today, flash is mostly used in environments where content such as video and video-like data is the bread and butter of the organization.

SSDs/HHDs

Lately, there has been a lot of talk that metadata is the new data. Whether this is true or not, using metadata to do backups, for example, has proven to be beneficial in many ways, but mainly the time it saves to complete a backup. Think of synthetic backups. SSDs and HDDs are contained inside disk arrays whether on site, in the cloud, or in your own DR site. Replication to a DR site can be considered as part of a tiered storage strategy to secure your data. Traditionally speaking, replicating your data to an offsite location has usually met the requirements for certain guidelines like GDPR. We will not go into details of what GDPR is, but there is plenty of information that can be found on the Internet. Replicating to a secondary disk array and then storing a cold copy in the cloud or on-prem tape is a good method of tiering your data.

Replicating to a secondary disk array and then storing a cold copy in the cloud or on-prem tape is a good method of tiering your data.

Tape

For its air-gap capability, tape is still on the list of top technologies to consider for security and data protection. Tape offers the most cost-effective method of protection against ransomware attacks. With its high-speed restore rates (currently with LTO-8 generation, up to 750 MB/s transfer rate), and capacity of up to 30 TB per LTO-8 cartridge, the cost per GB is outstanding. The economics to store large volumes of data for long-term retention while at the same time protecting your assets from ransomware leave no room for doubt that this old but resilient and cutting-edge technology still holds strong in data centers across the world. The usual drawback is that it is not as fast as disk. This is true, but when you consider the cost of storing cold data on spinning disk you will find there are significant savings that could be realized almost immediately—**such as a reduction in power, cooling, and data center footprint.**

Tape offers the most cost-effective method of protection against ransomware attacks.

CLOUD & OBJECT STORAGE

Public Cloud

Since the COVID-19 incident, the public cloud is looked at more favorably than it was in the recent past. How do we know this? Because if it were not for all those applications we are running in the cloud, there is a remote chance many of us would be able to work from home. The elasticity and economies of scale we can leverage are stellar under certain conditions. As IT spending shrinks, leveraging this technology can give you peace of mind, but without actual numbers it is hard to estimate what your real spend is going to be. Another thing that we learned during this COVID-19 incident is that the Public Cloud and SaaS providers were able to quickly increase their compute resources to accommodate the new demand. This is something that most enterprises, especially small ones, can't do quickly. The reasons go beyond funding. With COVID-19, we saw that supply chains were crippled and lead times on hardware increased dramatically. So even if an organization wanted to increase compute power in an on-premises data center, there was no equipment to be had quickly.

Hybrid Cloud

A hybrid cloud offers flexibility. Connecting your on-premise private cloud to a third-party cloud provider is considered a hybrid cloud in the most basic terms. It allows your compute and storage environment to share the workload and capacities available with the third-party cloud provider. Some of the benefits include choosing the most optimal resource for applications and the scalability to store multiple petabytes of data without having to make a capital expenditure.

Object Storage

Large unstructured data sets that need to be stored and protected forever should live in an object store. This solution makes it easy to manage, scale, and protect valuable data while providing the user with information to gain insight and extract value from its data sets. This is a benefit that can improve business outcomes because with object storage you can analyze massive amounts of unstructured files and object data. Lastly, object storage can be designed for extreme scalability such as exabyte-scale architecture, and it can meet the diverse needs of many industries where unstructured data sets are created at large scale.

Enterprise Applications in the Cloud

In a study of our own internal IT organization, we learned every employee is issued a portable computer—either a Windows-based laptop or a MacBook, depending on the needs of the user. The IT group also employs SaaS solutions like Microsoft 365. This provides collaboration tools like Microsoft Teams and Exchange Online as well as business productivity tools either online or installed on the laptop. In addition, many other Enterprise applications are SaaS based, meaning they are accessible from anywhere over the Internet. Example: CRM (SalesForce.com). Leveraging the public cloud in this scenario is a good cost-effective solution that enables a remote workforce effectively and efficiently.

Key Considerations for Applications in the Cloud

- Whether you decide to leverage the scalability and elasticity of the cloud, the demand for availability and storage will continue to be a constant as we look ahead.
- More and more enterprises will move partially to the cloud, enabling a hybrid cloud, while others will embrace a full-blown public cloud policy.
- CFOs across industries are charging their people to turn CAPEX purchases into OPEX and where it makes sense, it is ideal.
- One thing to remember is that not all data is created equal and it holds different value in all its lifetime.
- The benefit of the cloud is to be able to spin up and spin down resources, but the downside is you tend to lose control once your data leaves your premises—and never forget to account for those egress charges should you need to pull down data.
- All in all, shifting to an OPEX scenario with an on-prem and public cloud can be a life saver when/if all your security and availability requirements are met.

WHAT'S NEXT? JUSTIFYING TO YOUR CTO/CFO

We touched on a lot of different technologies that are, not only essential, but required if you want to achieve the security and resiliency of a modern and efficient IT infrastructure. Having the knowledge of what you need is only the first part. The second part is justifying to your CTO/CFO.

The following are recommendations for justifying essential technologies to your CTO/CFO:

- We recommend that you lean into your vendor for help justifying the cost effectively—ask for help.
- Know the value of the solution you are considering implementing and gather the data points necessary like the ROI/TCO information your C-level executive will require to make a decision. Your vendor will know the value of their solution better than anyone else, and they will also have case studies, which are similar to the challenges you're trying to solve.
- Leverage the tools available with your vendor to come up with your own analysis and remember, CFOs are now looking at projects through the lens of value and cost optimization, as together you work to digitally transform or shift to a post-crisis plan.

READY TO LEARN MORE?

For more information about Quantum Enterprise Backup and Archive solutions, visit:
www.quantum.com/data-protection

Quantum

Quantum technology and services help customers capture, create, and share digital content—and preserve and protect it for decades at the lowest cost. Quantum's platforms provide the fastest performance for high-resolution video, images, and industrial IoT, with solutions built for every stage of the data lifecycle, from high-performance ingest to real-time collaboration and analysis and low-cost archiving. Every day the world's leading entertainment companies, sports franchises, research scientists, government agencies, enterprises, and cloud providers are making the world happier, safer, and smarter on Quantum. See how at www.quantum.com.

©2020 Quantum Corporation. All rights reserved.

www.quantum.com
800-677-6268

ST02315A-v01 June 2020