

# BACKUP BASICS

Choosing the Right Data Protection System

Quantum

# TABLE *of* CONTENTS

**6**

**BACKUP  
BASICS**

**8**

**BACKUP OR PERISH:  
A HARSH LESSON**

**10**

**ESSENTIAL ELEMENTS  
OF A BASIC DATA  
PROTECTION SYSTEM**

**12**

**DISK AND TAPE  
DATA PROTECTION  
CONSIDERATIONS**

14

SELECTING YOUR  
DISK BACKUP SYSTEM

18

WHAT IS  
DEDUPLICATION

20

WHICH DISK-BASED  
SYSTEM IS RIGHT FOR  
ME? **RDX**

22

WHICH DISK-BASED  
SYSTEM IS RIGHT FOR  
ME? **NDX**

24

WHICH DISK-BASED  
SYSTEM IS RIGHT FOR  
ME? **DXi**

**26**

**SELECTING YOUR  
TAPE BACKUP SYSTEM**

**28**

**REMOVABLE  
MEDIA ROTATION**

**30**

**WHICH AUTOLOADER  
OR TAPE LIBRARY IS  
RIGHT FOR ME?**

**32**

**ENTRY-LEVEL  
LIBRARIES**

**34**

**THE BRAINS BEHIND  
THE HARDWARE**

**36**

**A QUANTUM  
SOLUTION TO FIT  
YOUR BUSINESS**

**38**

**WHAT YOU NEED  
TO KNOW BEFORE  
SHOPPING FOR A  
BACKUP SYSTEM**

**42**

**SO... HOW DO I  
INSTALL THE SYSTEM?**

**44**

**UP AND RUNNING.  
SO NOW WHAT?**

**46**

**IT'S TIME TO REVISIT  
JANE'S STORY**

**48**

**WHERE TO TURN  
IF YOU HAVE MORE  
QUESTIONS**

**50**

**GLOSSARY**

# BACKUP BASICS

**Are you responsible for making sure that the information on your company's network, servers or computers is safe and secure? Then this booklet is for you!**

Data is often the most important non-human asset that a company has. It represents the actual information and details behind the products and services that each company provides. If this data is lost, becomes corrupt, or is unavailable, it can have a major adverse effect on whether or not your company stays in business. Case studies have shown that up to 90% of small- and medium-sized businesses (SMBs) that suffer a major loss of data and have not sufficiently backed up their data will go out of business.

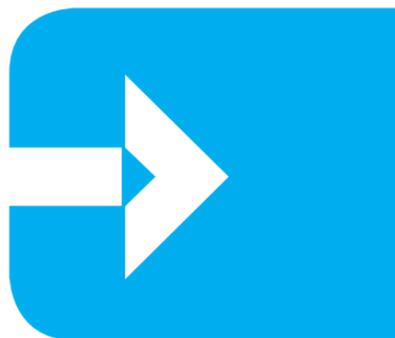
up to **90%**  
of SMBs that suffer a  
major loss of data...  
will go out of business

A solid data protection plan has three vital components:

- **Backup System:** This can be based on disk or tape, or a combination, along with appropriate backup software
- **Disaster Recovery Plan:** Off-site storage is a must, and data can be moved there either physically, by taking tapes or removable disks to another location, or electronically, by replicating over a network
- **Long-Term Archive:** Data that doesn't have to be immediately accessible can be stored on inexpensive media such as tape. The length of storage depends upon business needs and regulatory compliance.

### THIS COMMON-SENSE GUIDE

will assist you in selecting products that fit your data protection and disaster recovery needs. It also explains the tools that you will need to automatically and reliably make sure your data is safe.



# BACKUP OR PERISH: A HARSH LESSON

Emails continued to pour in. The phones kept ringing. And the light switches still made the office either light or dark. Dark was just fine with Jane. The business she built from the ground up was gone.

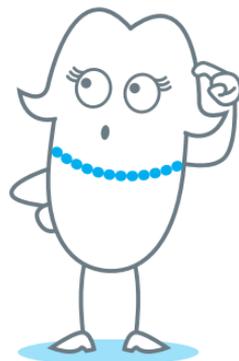
The previous night, burglars had stolen the company's desktop computers, servers and portable hard drives. Portions of Jane's finished projects had been copied to the hard drives. And she had printed copies of previous years' accounting and payroll data. But most of her current projects, billing information, email, and client and employee information were simply gone.

Sure, her insurance would replace the computers. It would even cover the expensive software that was central to her business. But insurance wouldn't replace the information that was stored on the computers.

Jane and her employees never felt they had the time to back up company information and files for safekeeping. And it never even occurred to them to back up something as common as email. Although she relied on technology to drive her business, Jane felt that a formal business data protection process and systems were too expensive, too “techie,” and overkill.

### Jane was wrong on all counts.

She found, as too many others before her, that the data on her computers actually was her business. Lose it and you may lose everything. Therefore, the question isn't, “How much does a data protection system cost?” It's really, “Can I afford not to protect my data?”



# ESSENTIAL ELEMENTS OF A BASIC DATA PROTECTION SYSTEM

When you start to look at creating a data protection process, it is valuable to know that every backup and recovery system has six essential elements:

## **DATA**

Digital information, especially information organized for analysis or used to make decisions, i.e., the content of your hard drives.

## **HARDWARE DEVICE**

Backup is simply copying data from one device to another with the intention of protecting it against loss or damage. You can back up to disk and/or tape appliances and solutions.

## **SOFTWARE**

An essential part of a data protection system is backup software. These applications specifically aid in automating the collection, tracking, and writing of data to a backup device, as well as the restoration of data from the backup device to its place of origin.

## **BACKUP PROCESS (INTERNAL BUSINESS PROCESS)**

Scheduling backup operations in a way that adequately protects data, while minimizing the impact of backup operations on networks, is critical. Properly established, the backup process can liberate a company from the chore of baby sitting the backups (i.e., most backups can take place after business hours).

## **OFF-SITE LOCATION**

Storing backup data (tapes or disks) in the same facility where it's created exposes your backups to the same risk as the original data (such as fire and theft). By either electronically replicating the backup to another site or making regular backup copies of that data via removable media (disk or tape cartridges) and periodically taking these backup copies to another location you can easily restore lost data if disaster strikes.

## **MEDIA**

If using removable media, then having the correct number of media cartridges (tapes or removable disks) on hand to support the backup device and backup methodology you select is critical. A solid media management plan promotes increased reliability and ensures media longevity.

# DISK AND TAPE DATA PROTECTION CONSIDERATIONS

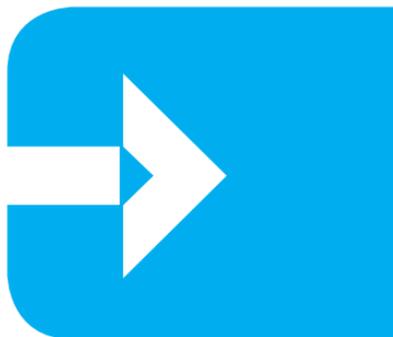
The right balance of disk and tape technologies can help you maximize performance, minimize total cost of ownership (TCO) and achieve a rapid payback. Here's an overview of each technology:

## **DISK-BASED STORAGE**

has the advantage of being random access (i.e., the drive goes directly to the file you are seeking) versus the sequential access of tape (i.e., the drive must run the tape until it reaches the location of the file), thus making file restores quicker. It is also less likely to become obsolete, since disk standards are long-lived and are backward-compatible to many older generations. Some disk systems also have the advantage of using data deduplication (not available with tape), which dramatically reduces the amount of disk space used when storing backup data.

## MAGNETIC TAPE

is still the lowest overall cost per gigabyte for storage and one of the most portable media for high capacity needs. It is also immune to computer viruses, and data is typically stored in a compressed format, effectively doubling the capacity of each tape over native format. Tape cartridges easily fit in the palm of your hand, and the data transfer rate is so fast on some tape drives that they can back up multiple servers at once. In addition, tape is uniquely “green,” since the drive motor only runs when a backup or restore operation is in progress. Archived tapes have a very long shelf life (20 years or more).



# SELECTING YOUR DISK BACKUP SYSTEM

A small- or mid-sized business that chooses to use hard disks as the primary backup system generally has three choices of technology: removable disk, network-attached storage (NAS) or a dedicated backup appliance.

A [removable disk](#) is a ruggedized hard drive that is contained inside a sealed cartridge shell which includes shock-mounting so the disk can survive typical office accidents such as dropping it on the floor. The interchangeable cartridges come in multiple disk capacities and can be inserted either into a standalone dock, which holds one cartridge at a time, or a disk library, which can hold multiple cartridges and automatically manages where the data is stored or retrieved.

A [network-attached storage \(NAS\)](#) system is a dedicated storage computer that contains multiple hard drives. It can be used either for primary storage or backup, depending upon the software that is installed. When NAS is used with backup software, the primary data is pulled over the local network and saved for quick and easy recovery as needed.

A [dedicated backup appliance](#) is similar to a NAS system except it has been designed specifically to be a backup target, providing much higher performance and typically has proprietary software or onboard hardware that optimizes the backup process. Two features often available with such a backup appliance are the ability to efficiently protect virtual machines and the capability of being part of a larger-scale data protection system.

## **DISASTER RECOVERY BEST PRACTICES FOR NAS AND BACKUP APPLIANCES**

Multiple copies of backup data maintained at separate locations are required to adequately protect data from disasters like fire, theft, flood, etc. When using fixed disk solutions like NAS and dedicated backup appliances for data protection, there are several options for disaster recovery.

### **REPLICATION TO A SECOND SITE**

Replication (copying data) from one disk system to another is suitable for customers with multiple sites. Using capabilities of the appliance or software, data is replicated from the backup appliance over the WAN (wide area network) to another appliance at a second location. It is best if this second location is a significant distance away from the first location, so that a natural disaster like earthquake or flood at the first location does not also impact the second location.

## REPLICATION TO CLOUD

Customers may choose to replicate data to a service provider, also known as the cloud. This provides the protection of replicating to a second site but is financed like a service, typically on a monthly basis, with no need to buy hardware (or have a second site). Data is typically sent over a secure VPN (virtual private network) to the service provider's data center.

## COPY TO REMOVABLE MEDIA

Customers may choose to back up to disk and then copy the data to removable media (tape or removable disk cartridges) for disaster recovery. Cartridges are then rotated off-site to another location or service provider for protection against a disaster at the first location off-site.

# WHAT IS DEDUPLICATION?

As your backup data grows, disks tend to fill up, requiring you to either delete some of your older archived data to make space available or add more disk capacity. Standard backup software helps somewhat by saving only files that have changed since previous backups, but that is somewhat inefficient because if you change one word in a document, the entire document is still backed up again.

A better solution is called data deduplication. The software looks inside files that are about to be backed up, finds the parts that have changed since the previous backup and saves just that component. When you want to retrieve the backed up file as it looked on a certain date, the software intelligently reconstructs the file, putting all the changes in the right places, and presents you with the version you requested. As a result, a great deal of disk space is saved (sometimes as much as a 20:1 reduction, depending upon the types of files and how often they have been modified).

Data deduplication can be done several ways, with varying degrees of sophistication and granularity. Smaller-scale systems may perform the deduplication on each file separately. Thus, if the same file resides on multiple machines or standard components are used repeatedly, each instance will be treated separately.

More powerful deduplication systems are more granular and can detect if small components (blocks) are being used in multiple files or on multiple machines. They save even more disk space by using pointers to the common components rather than resaving data that is already stored in the system. In addition, such software can work with existing backup applications so a company can standardize across all backup systems, including both disk and tape.

Data deduplication saves time and money while allowing customers to keep more data on their system. Also, because data growth is controlled, customers spend less money on new disk capacity and upgrading hardware due to space limitations.

In addition, backups happen more quickly because only changed data is saved. A full backup occurs only once, when the appliance is new, and every backup after that is only an incremental.

Deduplication provides critical benefits for replication to another appliance or the cloud. Replicating deduplicated data consumes very little bandwidth, which can be critical when sending only changed data over a WAN or VPN, which may be slow and can be expensive.

# WHICH DISK-BASED SYSTEM IS RIGHT FOR ME? RDX

## RDX SERIES REMOVABLE DISK

The Quantum RDX® (standalone) and RDX 8000 (8-slot library) are removable, disk-based data protection solutions for small- and medium-sized businesses. They combine the best features of disk—fast access and fast restores—with the best features of tape—removability for disaster recovery and an easy-to-use backup process.



## RDX 8000

Backups are to removable, industry-standard RDX cartridges that can then be taken offline or off-site

Multiple, interchangeable cartridge capacities let you easily scale up as your data grows (currently up to 1TB native capacity per cartridge before deduplication)

RDX 8000 features iSCSI connectivity and disk or tape emulation mode

RDX 8000 is available with Quantum DATASTOR Shield™ client-side deduplication software (or without, for use with all major backup software packages)

Standalone RDX includes GoProtect™ deduplication software

RDX 8000 is centrally managed from the backup server through a simple, easy-to-use Windows interface



# WHICH DISK-BASED SYSTEM IS RIGHT FOR ME? NDX

The Quantum NDX Series of network-attached storage (NAS) appliances for backup, disaster recovery and primary storage offer a complete storage and data protection solution for small and medium businesses.

The NDX-8d and NDX-12d Data Protection Appliances utilize client-side deduplication, to hold 5x more data than non-deduplicated NAS, while reducing network traffic by 90%. Operations are centrally managed through the NAS, and there are no software agents to install on clients being backed up (agentless). The NDX-8d and NDX-12d back up Windows systems including desktops, servers, virtual machines, Exchange, SQL Server and SharePoint.

The Quantum NDX-8 and NDX-12 NAS are designed for primary storage and boast more powerful processors and RAM than competitors, while featuring enterprise-class hard drives for ultimate speed and RAID reliability. NDX offers true business class storage that fits the budget of small and medium businesses.



## NDX-8d and NDX-12d

### *Data Protection Appliance with Deduplication*

Protects two years of data or more, while maintaining greater history than tape or other disk

Controls data growth, reducing the amount of data stored and network traffic by up to 90% through deduplication

Centrally managed from the NAS unit through a simple, easy-to-use interface

Comes standard with easy to use DATASTOR Shield deduplication software

Agentless backup – no software to install on the clients

Designed for Windows environments



## NDX-8 and NDX-12 NAS Storage

Business class storage for networked environments

Use as a file server or as iSCSI direct attached storage

Faster, more reliable with Intel Dual Core i3 3.3GHz processor, enterprise-class HDDs and 4GB of RAM

Compatible, consistent Windows storage server operating system

Available in a tower or 1U rackmount configuration

# WHICH DISK-BASED SYSTEM IS RIGHT FOR ME? DXi

## **DXi4000 SERIES BACKUP APPLIANCES**

The DXi4000 Series appliances are designed to provide small to medium sized businesses and branch offices with high-performance data protection at an industry-leading price. With them, you can add powerful deduplication to your existing architecture simply and without disruption. They integrate easily with all leading backup software and can be linked to larger DXi® units at the data center to centralize data protection and archiving to tape libraries.



## DXi4701

*Affordable, high-performance deduplication appliances featuring Capacity-on-Demand scalability for fast, easy growth. Scalable capacities from 5-135TB usable.*

The DXi4701 offers Capacity-on-Demand (CoD) scalability from 5-135TB by simply activating a license key—scalability with no additional hardware to purchase or install

Provides up to 5.0TB/hour native performance faster than leading competitors

Reduces typical disk capacity needs by 90% or more through deduplication

Integrates smoothly with all leading backup applications, including NetBackup and Backup Exec



# SELECTING YOUR TAPE BACKUP SYSTEM

Most small or mid-sized businesses that choose tape to either back up their primary storage or complement existing disk backup appliances will want an autoloader or automated tape library solution.

The terms “autoloader” and “library” refer to an automated backup device that contains tape drive(s), slots for holding tape cartridges and a robotic mechanism for moving tapes between the slots and the tape drive(s). They are controlled by backup software, enabling specific backup routines to run automatically while simplifying restoration of data, and can usually be configured and monitored remotely via a web browser or other software. Both typically contain bar code readers to help with management of the tape cartridges. An autoloader contains a single tape drive, while a library has the capability of holding multiple tape drives that can run simultaneously to speed the backup process.

## WHAT ARE THE ADVANTAGES OF AUTOMATION?

### “LIGHTS OUT” BACKUPS

For best performance and efficiency, backups are typically run overnight, during the 8 hours or so when your staff isn't actively using the computer network. If the data to be backed up doesn't fit on a single tape, either because the size of the backup job wasn't scoped correctly or part of the media was already used by a previous job, the backup software asks for another tape. In the case of a single standalone drive, this means the backup job stops until a new tape is manually inserted... and most likely, nobody will be there to do this. With an autoloader or library, the device handles this chore and the backup continues to completion.

### MEDIA ROTATION

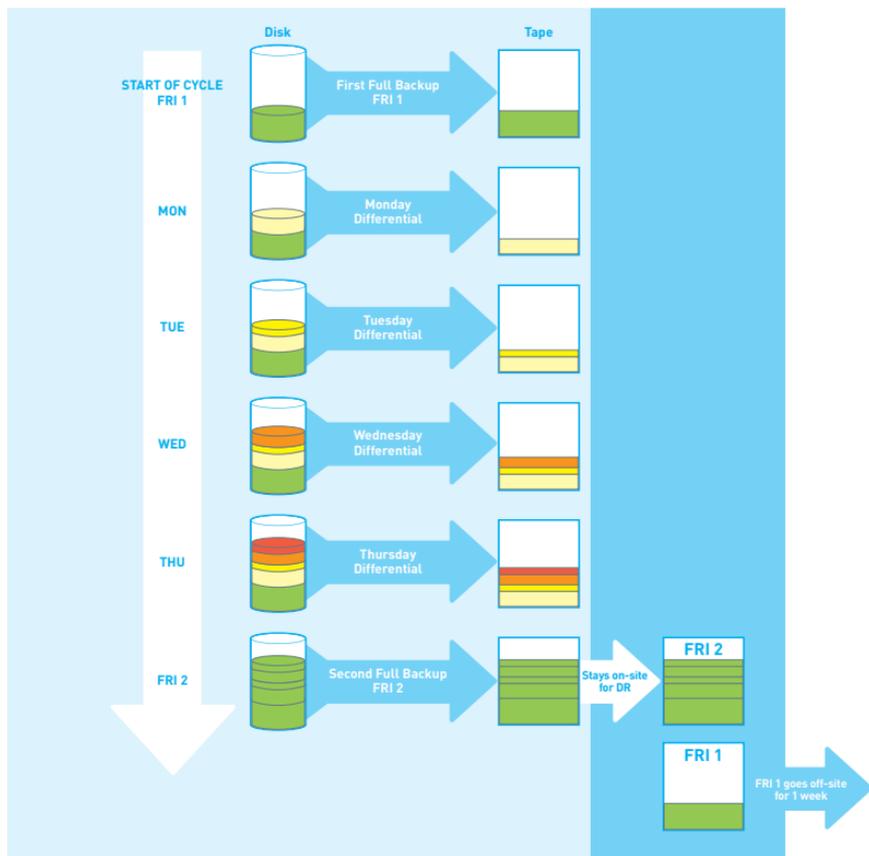
With removable media, the best way to protect your valuable business data is to perform a backup of new data every night, dedicating a separate tape to each week or day of the week. The media are “rotated” in sequence, one after another, so that new data doesn't overwrite older data in case you need to go back several days or weeks to find a particular version of a file someone has been working on. By loading tapes or removable disks into multiple slots of an autoloader or a library, this rotation does not require manual intervention, unlike a standalone drive that only holds one tape or disk at a time. Eventually, media are removed from the rotation system and stored off-site for a period of time in order to maximize the disaster recovery ability; a new set (or recycled older ones) is then loaded into the system.

# REMOVABLE MEDIA ROTATION

The illustration on the right shows an example of a media rotation scheme using tape cartridges or removable hard disks without deduplication. This blends maximum data protection with fast data recovery.

The six-cartridge weekly backup is perfect for small businesses. This backup principle requires daily backups and a single weekly off-site backup copy to provide a data history of up to two weeks. Friday backups are full backups. Monday through Thursday backups just save the new and changed data.

## Six Cartridge Weekly Backup Cycle



# WHICH AUTOLOADER OR TAPE LIBRARY IS RIGHT FOR ME?

## SuperLoader 3

Selecting an autoloader or entry-level tape library is fairly straightforward. Determine how much total data you need to back up now and how much excess capacity you want on hand to allow for data growth in the future. You certainly don't need to fill all the tape slots with cartridges unless you want to.

Automating the backup process is easy and affordable with Quantum's entry automation solutions. Quantum's SuperLoader® 3 autoloader and Scalar® i40/i80 tape libraries provide proven, highly reliable, and cost-effective solutions versus standalone drives to help small- and medium-size businesses protect their data.



## SuperLoader 3

Contains a single tape drive

8 or 16 tape slots in removable magazines

Compressed data capacities range from 13TB to 48TB\*

A variety of tape drives are available, including LTO-5 with native encryption

Available interfaces are SCSI and SAS and native FC interfaces

Includes remote configuration and monitoring

*\*Assumes industry-standard 2:1 compression*



# ENTRY-LEVEL LIBRARIES

## **Scalar i40/i80 Tape Libraries**

You have many choices for hardware and your selection should be based upon your budget, amount of data and the backup time window. Be sure also to consider the stability of the manufacturer, experience in backup/recovery and breadth of product lines.



## Scalar i40/i80

Intelligent tape library that is ideal for small-to-medium businesses and remote office environments

Scalar i40 expands from 25 slots to 40 slots, holds up to 2 drives.  
Scalar i80 expands from 50 slots to 80 slots, holds up to 5 drives

iLayer™ intelligent management software simplifies library management and increases reliability, reducing service calls by 50%

Capacity-on-Demand (CoD) growth for simple, non-disruptive expansion, providing market-leading investment protection

AES 256-bit encryption is standard for the highest levels of security

SAS and native Fibre Channel interfaces available



# THE BRAINS BEHIND THE HARDWARE

Choosing a backup device or an autoloader/library is only part of a backup solution. You must also decide which backup software you will use to control the device. Software can be simple, backing up just the files on a single server, or it can be complex, protecting multiple servers along with email systems, databases, etc.

Backup software collects data from various sources, such as PCs and file servers, and writes a copy of that data to the tape or disk in the backup device.

Autoloaders, libraries and backup appliances respond automatically to commands from the backup software. Human intervention is only necessary when inserting and removing media from the autoloader or library, such as for off-site storage purposes. Backup routines and tape drive-cleaning regimens can be managed by the backup software, so data is protected without hassles.

Backup software products from Independent Software Vendors (ISVs) are highly refined and are often optimized to work with specific models of backup devices.

## QUANTUM PRODUCTS AND BACKUP SOFTWARE

All of Quantum's products are compatible with all major backup software packages, including but not limited to:

- Symantec with Backup Exec™ and NetBackup products
- EMC with NetWorker
- Computer Associates (CA) with ARCserve®

In addition, several of Quantum's products come with their own software, which replaces or enhances traditional backup software.

# A QUANTUM SOLUTION TO FIT YOUR BUSINESS

Quantum offers complete solutions for both physical and virtual data protection. The integration of industry-leading software technology with complementary hardware provide simple, turnkey solutions designed to meet your performance and capacity needs today and into the future as your business grows. All our solutions include deduplication technology to control data growth and protect your investment over time.

## **QUANTUM vmPRO SOFTWARE**

Unlike traditional backup applications and other backup applications designed for virtual environments, Quantum vmPRO™ Software backs up VMs in native VMware format, enabling users to restore or boot VMs in seconds without the use of a backup application; reduces virtual server and network usage by reducing VM image sizes before backing up those images to backup storage; and substantially reduces the cost of using traditional backup applications to back up virtual environments.

## **QUANTUM DXi V-SERIES**

Quantum DXi V-Series is the first solution in the industry to combine the power and flexibility of target-based deduplication with the simplicity and affordability of a virtual appliance, using the IT infrastructure already in place without sacrificing performance. DXi V-Series works with any backup software to store up to 360TB of data on any physical and virtual servers, just like a physical deduplication appliance. For DR protection, it can replicate to any other DXi appliance—DXi V-Series included—or to a cloud protection service like Q-Cloud™.

## **QUANTUM NDX-8d, NDX-12d AND RDX 8000 WITH DATASTOR SHIELD DEDUPLICATION SOFTWARE**

These solutions come complete with hardware and software that performs deduplication on Microsoft Windows systems. Simple licensing and warranty terms make this a cost-effective solution when compared to purchasing backup software and hardware separately. For this solution, no additional backup software is required. However, for customers wanting to use their existing backup software, the NDX-8 NAS, NDX-12 NAS and RDX 8000 are also available without the DATASTOR Shield deduplication software and work seamlessly with all major backup software packages.

## **QUANTUM RDX STANDALONE DRIVES**

RDX standalone docks are compatible with backup software from the major brands; however, the GoProtect deduplication software is included with each RDX dock. GoProtect will perform a deduplicated backup of a single Microsoft Windows desktop, laptop or server, with the ability to back up Exchange, SQL and Sharepoint.

# WHAT YOU NEED TO KNOW BEFORE SHOPPING FOR A BACKUP SYSTEM



## WHAT IS YOUR BACKUP WINDOW – WHEN AND HOW LONG WILL IT TAKE YOU TO DO YOUR BACKUP?

Since the backup process is touching the data while it is making a copy, as well as taking up network bandwidth, it is recommended that you back up your data after your employees have gone home. That way work is not affected by the load on the file server or the network. So, if your company is like most, you can start your backup at 8 pm. If you want it to finish by 6 am the next morning, you have a 10-hour backup window.



## HOW MUCH DATA DO YOU NEED TO BACK UP?

Typically, you will only need to back up your live data, rather than everything on your computer such as program files and the operating system. To see how much data you have on a Windows-based system, you can look in your application data folders and the 'My Documents' folders. Most computer operators know how to see how much data is on the hard drives.

Most days, you will only need to back up the data that has changed since the previous backup. There is no need to back up data that has not changed when you already have a copy of it in your full backup.

With tape or non-deduplicated removable disk, full backups generally occur each week, overwriting a prior full backup, with other days backing up only changed data (incremental).

With fixed disk and deduplicated disk (removable or fixed), a full backup occurs once and then all subsequent backups store only changed data. Periodically, past backups are retired (deleted) using functionality in the software, to free up disk space. An example is to keep 30 days of daily backups, weekly backups for the most recent year and monthly backups for prior years.

For example, using tape or non deduplicated disk, where 5% of the data changes each day (actually, this is a large amount), a schedule might look like this:

Friday Full Backup: 1.5TB – compressed 2:1 to 750GB

Monday - Thursday Backup: 75GB – compressed to 37.5GB

Friday Full Backup: 1.5TB – compressed to 750GB

Given 2:1 compression capability with most tape and backup software, you would need a cartridge that can hold your largest backup – i.e.  $1.5\text{TB}/2 = 750\text{GB}$ . For tape, this would be an LTO-4 (800GB) or LTO-5 (1.5TB) cartridge. We would recommend LTO-5 to allow for several years of room for future data growth.

If you are using a disk-based system with data deduplication, the amount of disk space used can be dramatically less. Full backups typically achieve 2:1 data compression, but are only done once. All subsequent backups are daily incrementals and reductions of 20:1 or greater are possible depending on data type.

The same example with deduplication looks like this:

Friday full backup: 1.5TB – compressed 2:1 to 750GB

All subsequent backups: 75GB – deduplicated 20:1 to 3.75GB

So for deduplication, a good rule of thumb, given normally compressible data, is to purchase a disk system or cartridge that has 1.5 to 2x the capacity of your full backup. For a 1.5TB backup, you would want 2.3TB to 3TB of capacity to allow space for future backups and data growth.



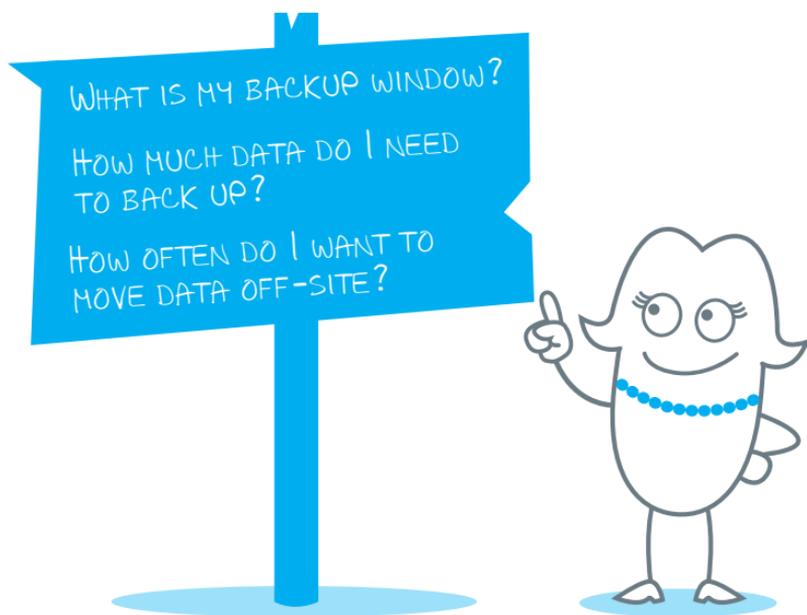
### HOW OFTEN DO YOU WANT TO PHYSICALLY MOVE DATA OFF-SITE?

Remember that you will want to have your data stored in another off-site location to prepare for a worst-case scenario in which all of your computer data is lost, such as a fire.

If you move physical media (tape or removable disk) off-site every week, your data would be at most one week old. Can you afford to lose a week's worth of data? Only you can answer that. During normal backup operations, you can "recycle" these cartridges in

a rotation scheme, overwriting them after a sufficient number of more recent backups has been made, unless you have a regulatory requirement to keep all the data.

If you are using disk systems and have a remote site available, you can replicate data electronically to another system, using a wide-area network (WAN) or a VPN through the Internet. This can be done daily, especially if the data is deduplicated, and usually is an automated process. Quantum's DXi and NDX appliances are especially suited for such replication.



# SO... HOW DO I INSTALL THE SYSTEM?

When you purchase a backup device, autoloader or entry-level library, you will receive full installation instructions or some type of “Getting Started” guide. Fortunately, one of the central missions of manufacturers is to make their products easy to install and use. Installation guides are typically simple documents that contain graphically detailed instructions in easy 1-2-3 order.

Special skills or knowledge of computers is not absolutely necessary, but it may help. In general, you can expect the following for installation steps:

## **CONNECTING THE DEVICE TO A SERVER OR NETWORK:**

If your server doesn't have the proper connection port, you may need to install an interface card, also called a host bus adapter (HBA), to connect the cable from the drive, autoloader or entry-level library. Contact your computer professional for assistance if necessary.

### INSTALLING SOFTWARE:

At a minimum, this may mean the “driver” software that enables communication between the computer operating system and the device, although many backup devices are natively supported by Windows. You will also need to install backup software, either provided with the backup device or purchased separately. Both of these installations are generally straightforward.

### POWERING UP:

In the case of an external device, such as an autoloader, entry-level library or tabletop tape drive, you will need to plug it in and turn it on. There may be a simple configuration routine to perform with the user interface (screen and buttons) on the front of the unit.

### RACK-MOUNTING:

This one’s optional, but most autoloaders, entry-level libraries and data protection appliances (as well as some tape drives) are installed in a standard 19-inch equipment rack, using a rackmount kit. This might be handy if you want to put your backup system into the same rack as your servers.



Some people are not comfortable installing and configuring unfamiliar hardware and software. Make sure the manufacturer or reseller you purchase from offers installation services and adequate support.

# UP AND RUNNING. SO NOW WHAT?

Setting proper backup procedures is critical for maximizing the value of your backup solution. Most backup software will contain recommended procedures based on your needs. However, there are a few simple guidelines, as mentioned earlier in this guide.

## **HOW OFTEN?**

Most companies find that a daily incremental backup, with a full backup on the weekend, provides the right balance between data protection and impact on network systems.

## **HOW DO I KNOW IF IT WORKED?**

Backup software provides a “verify” function. It takes a little longer for the software to check the data it has written, but you’ll know it’s there when you need it.

## **DISASTER RECOVERY STRATEGIES**

All companies—of all sizes—need to store their backed up data off-site. That way, if there’s an earthquake, flood, fire, theft, virus or other disaster, data from the remote location can be returned to restore downed systems.

If you are using tape or removable disk, be sure to rotate the media on- and off-site on a regular basis. If you are backing up to a hard disk system, you can:

- Copy to tape on-site and then remove the tape to an off-site location; or
- Replicate from the on-site disk to an off-site disk installation via a WAN. This off-site information could then be copied to tape for lower-cost archived storage.

### **A BACKUP FOR YOUR BACKUP PROCESS**

Make sure that a second person is trained in the backup process in case the primary person is out of the office. It's also a good idea to periodically check backup tapes or removable disks to make sure that proper processes are being followed. When data is missing, it's usually not the hardware nor the backup software that's at fault!



Planning your backup process is the most important step in protecting your data.

# IT'S TIME TO REVISIT JANE'S STORY

Backup products like autoloaders, entry-level libraries and NAS appliances, help ensure happy endings to stories of near-tragedy. So let's visit Jane again, this time a month before the burglary.

Having read a copy of "Backup Basics," Jane had called her local reseller, whom she's trusted for years. She discussed her requirements and preferences with a salesperson and ordered a removable disk library with deduplication backup software.

Installation was easy. She scheduled daily backups and every Friday took home a removable disk containing the latest data. A system at the office contained a second copy of the backup and continued to backup emails and anything else that changed over the weekend. This, she decided, was adequate disaster protection for her company at its current size.

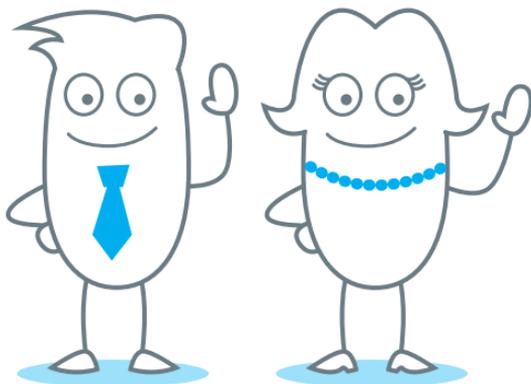
Disaster struck again. Burglars made off with all her office equipment, including her removable disk library.

But panic did not set in. Insurance claims were filed, equipment was replaced and, most notably, Jane's business did not fail. After pulling the removable disk containing the previous week's backups from her fireproof safe, Jane started to rebuild her systems, including data from client projects, contact databases, graphics archives and email. She and her employees settled in and picked up where they left off. Only two days' work was lost (she only brought home a copy once per week), but more than enough information had been recovered to easily recreate it.

Even if the burglars had never struck, the automated backup system streamlined her day-to-day operations by safely and routinely backing up data without human intervention.

That way, even common—but still troublesome—events, such as a hard drive failure, corruption from a virus, or mistakenly deleted files, could be managed without serious disruption to the business day.

Installing and maintaining a data protection system gave Jane's story a much happier ending this time.



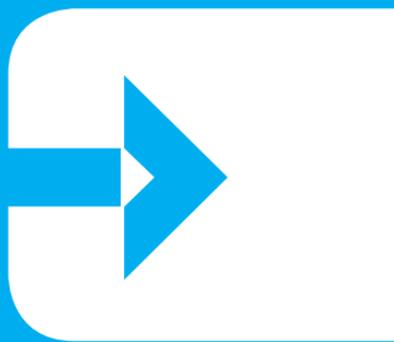
# WHERE TO TURN IF YOU HAVE MORE QUESTIONS

While “Backup Basics” is intended to answer many of the questions faced by businesses with backup challenges, it is not a replacement for individual contact with a knowledgeable storage professional.

Personalized help can be found at Quantum Corporation. Quantum offers field-proven and award-winning data protection solutions, and with more than 30 years of experience, is a useful resource for more detailed storage information.

For more product information and a list of Where to Buy, please visit [www.quantum.com](http://www.quantum.com).

In North America, you can also talk with a product representative in the Quantum Call Center, **toll-free at 866-809-5230**.



# GLOSSARY

**AUTOLOADER:** a data storage device containing one tape drive, tape cartridge slots and a mechanical device that automatically loads and removes tapes from the drive(s), usually used for backup/restore.

**AUTOMATION:** the techniques and equipment used to achieve automatic operation or control, i.e., replacing human activity with a mechanical solution.

**BACKUP:** the act of deliberately collecting data, creating a viable copy of it, and storing it where it is both safe and easily retrieved.

**BACKUP PROCESS:** the guidelines or schedules by which backup operations occur.

**BACKUP SOFTWARE:** a software application that specifically aids in automating the collection and writing of data to a backup device, as well as the restoration of data from the backup device to its place of origin.

**BACKUP WINDOW:** the time during which a backup is scheduled to take place, usually during non-working or off-peak hours when impact to network users will be minimal.

**CAPACITY:** the measure of data that can be stored on a device.

**COMPRESSION (COMPRESSED):** encoding data to take up less storage space on magnetic tape. Compression is carried out in the server (software compression) or in the drive itself (hardware compression). Software compression speed is dependent on computer processor power, whereas hardware compression gives optimum performance and is transparent to the user. Data transfer speed and total tape capacity are affected by the data compression achieved.

**DATA PROTECTION:** the act of reducing risk to data loss or corruption.

**DEDUPLICATION:** a sophisticated process for backups on hard disks that ensures data changes are only backed up once. This can reduce the amount of disk space consumed by up to 20:1.

**DISASTER RECOVERY:** a plan by which backed-up data can be restored after a catastrophic event.

**FULL BACKUP:** a backup operation that copies all available data from network-attached sources (servers, PCs, drives and drive arrays).

**GB:** gigabyte; a unit of computer memory or data storage capacity equal to one billion bytes (1000 megabytes).

**HOST BUS ADAPTER (HBA):** a hardware device, typically a plug-in card, used for the interface between a server and network or other device (such as an autoloader).

**INCREMENTAL BACKUP:** a backup operation that detects and collects only data that has been created or changed since the previous backup.

**INDEPENDENT SOFTWARE VENDOR (ISV):** software companies that create products to be used with hardware devices from various manufacturers. (e.g., Symantec, Computer Associates).

**LIBRARY:** a data storage device containing one or more tape drives or disk drives. In the case of tape, it contains multiple tape cartridge slots and a mechanical device that automatically loads and removes tapes from the drive. In the case of disk, the communication with multiple disk drives is done through software rather than mechanical means.

**NAS, NETWORK-ATTACHED STORAGE:** a self-contained, small computer appliance dedicated to primary or backup storage on disk. It is attached directly to the local area network, usually by an Ethernet connection.

**OFF-SITE:** a term used to describe the removal of backup tapes from the premises where they were created to provide a geographical safeguard against loss or damage.

**REMOVABLE DISK:** a ruggedized hard drive that is contained inside a sealed cartridge shell which includes shock-mounting. The disk can be removed from the backup device for off-site storage.

**RESTORE, RESTORATION:** to replace lost or damaged data with a copy found on a backup tape or tapes.

**SAS:** Serial Attached SCSI, the most advanced and highest-performance version of the SCSI interface.

**SCSI:** Small Computer System Interface; used for connecting peripheral devices, such as autoloaders, to computers or servers.

**STORAGE:** a place where data resides; example: server or computer hard drive, CD-ROM, DVD, magnetic tape.

**TB:** terabyte; a unit of computer memory or data storage capacity equal to 1,000 gigabytes.

# NOTES

# NOTES

# NOTES

# NOTES



## ABOUT QUANTUM

Quantum is a proven global expert in Data Protection and Big Data management, providing specialized storage solutions for physical, virtual and cloud environments. From small businesses to major enterprises, more than 100,000 customers have trusted Quantum to help maximize the value of their data by protecting and preserving it over its entire lifecycle. With Quantum, customers can Be Certain they're able to adapt in a changing world – keeping more data longer, bridging from today to tomorrow, and reducing costs. See how at [www.quantum.com](http://www.quantum.com).

[www.quantum.com](http://www.quantum.com) • 1.866.809.5230

©2014 Quantum Corporation. All rights reserved. Quantum, the Quantum logo, DXi, DXi Accent, iLayer, Q-Cloud Quantum vmPRO, Scalar, StorageCare and StorNext are either registered trademarks or trademarks of Quantum Corporation and its affiliates in the United States and/or other countries. All other trademarks are the property of their respective owners.



**BE CERTAIN**