Data Protection

IMPLEMENTING AN EFFECTIVE DATA PROTECTION STRATEGY BEGINS WITH EVALUATING THE VALUE OF YOUR COMPANY'S DATA AND THEN DETERMINING THE PROPER SET OF BUSINESS REQUIREMENTS FOR PROTECTING IT.

Evaluating Business Requirements & Classifying Your Data

The business of business is business, not IT. Your data protection practices, like your other business practices, should be aimed at managing your business assets because a simple analysis of your data can produce extraordinary results. This paper discusses an approach to evaluating data at a business level, and implementing a data protection strategy that safeguards your organization based on the value of its data.

Overview

Protecting your company's data and applications means much more than just running a simple backup routine. It is about protecting your business assets throughout their lifecycle – in terms of preservation, recoverability and availability. A sound data protection approach can help your company adapt more rapidly to its changing and increasing opportunities. For example:

- It can help ensure that your applications are continually in operation, serving your customers, and enabling your business.
- In the event of a file loss or disaster, it can minimize the length and severity of the disruption.
- It can support cost-effective compliance with regulations, reducing business risk and the cost of compliance.

Implementing an effective data protection strategy begins with evaluating the value of your company's data and then determining the proper set of business requirements for protecting it. A fairly simple approach is based on the frequency of change and the business criticality of data. Simply put, data that is mission-critical to your business requires a more robust data protection solution, and requires more frequent protection. This is a sound approach no matter how much data you have.

Only by first thinking about your business and the value of the data it relies on can you begin to define the requirements of an effective data protection solution in terms of application and data availability – as well as your IT budget.

AN EASY WAY TO DETERMINE WHAT DATA IS MISSION-CRITICAL IS TO SIMPLY ASK YOURSELF, AS WELL AS OTHER CROSS-FUNCTIONAL DEPARTMENTS, "WHAT HAPPENS IF THIS APPLICATION GOES DOWN OR DATA IS LOST? WHAT HAPPENS IF WE CAN'T GET IT BACK IMMEDIATELY?"

Managing Your Data

Frequency of Change: Dynamic vs. Static

Think for a moment about your data and its value to your business. Like almost every other company in the world, you probably have files you access and change every day. For example, when you use your ERP system or accounting package, every time you record a new invoice or payroll transaction, the data changes. This is called dynamic data.

You probably also have files that don't change once they are created. An example might be a proposal you just wrote for a new customer. Once you have created and delivered it, the file probably will not change. This is called static data. Other examples include engineering drawings, maps, pictures, x-rays, video, presentations, etc. If you consider it, you will probably realize that you have more static data than dynamic data. If so, you are not alone because this is true for most businesses today.

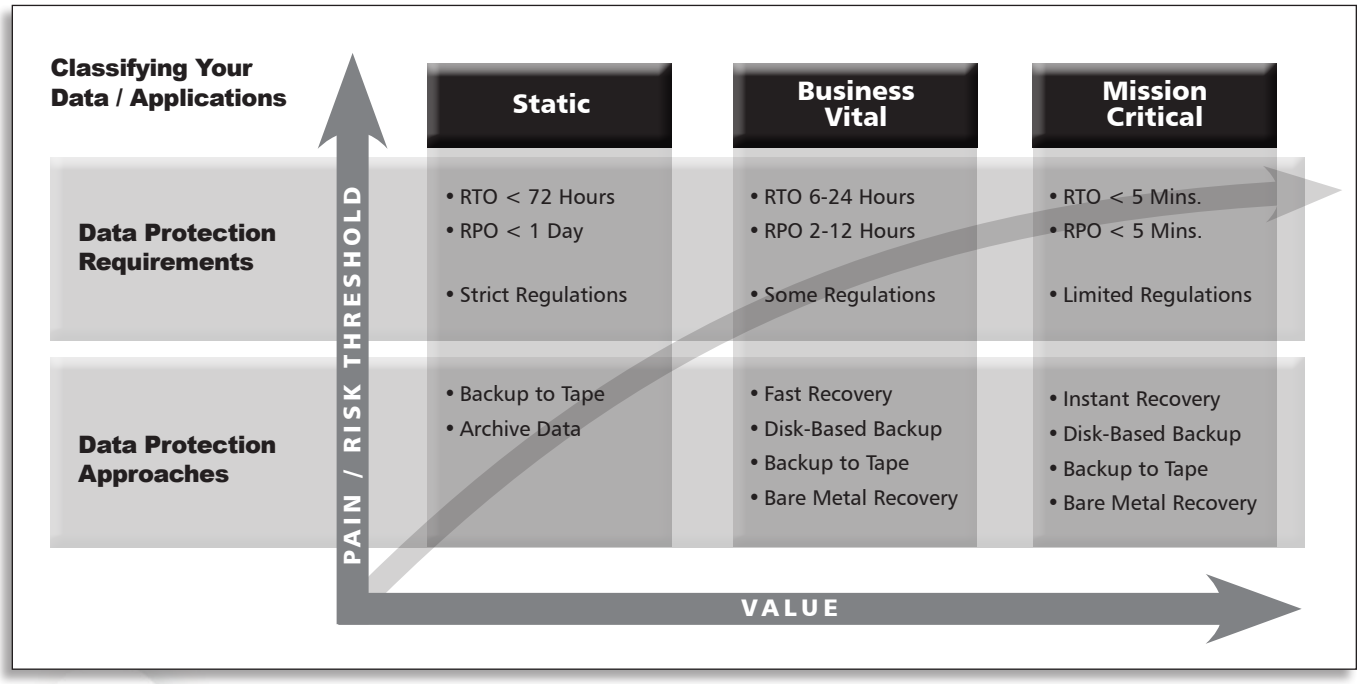
Business Criticality

Another dimension to think about when considering your data is its importance or value to your business. Some data is clearly "mission-critical" – in other words, your business will be damaged if you lose it; you could lose revenues or be running legal risks, etc.

Which data is critical depends on your company. For some, email is critical; others consider their accounting, customer, or supplier data to be critical. An easy way to determine what data is mission-critical is to simply ask yourself, as well as other cross-functional departments, "What happens if this application goes down or data is lost? What happens if we can't get it back immediately?"

More than likely, you also have data that is not critical. This typically includes things like the three versions of that presentation you saved before you considered it ready to go, or your marketing collateral, etc. It's unlikely your firm will cease operating if you can't access this data for a brief period.

Data Protection Approaches



IF YOU TAKE TIME TO UNDERSTAND YOUR DATA AND DEFINE YOUR BUSINESS REQUIREMENTS ACCORDINGLY, YOU CAN GAIN SIGNIFICANT BENEFITS.

Steps to Defining Your Data Protection Strategy

As we have discussed, the key to implementing an effective and efficient strategy for properly protecting your data is to first analyze and determine its value to your organization. Only then can you establish a clear set of business requirements for protecting it. If you take time to understand your data and define your business requirements accordingly, you can gain significant benefits. Doing it properly means that you can have high application availability to help your people serve your customers and help your customers serve themselves. It means you can limit disruptions. And it means you can retrieve data to meet compliance requirements or for repurposing in new applications.

1. Define a set of "data classes"

Data classes are groups of data that have similar criticality to your business and also similar frequency of change. You do not want to have a different data protection approach for every data set that you have. Grouping your data into classes with similar characteristics will allow you to implement a less complex strategy.

As discussed earlier, the easiest way to classify your data is to define the criticality and frequency of change for all of your major data sets and look for commonalities in the results. Classifying data in a vacuum based on assumptions may come back to bite you. Be sure to get others (e.g. business line managers, support staff, etc.) to participate in this exercise. You will undoubtedly have to make some trade-offs in order to limit the number of data classes you have. For medium-sized businesses, the number of classes should likely be between three and five.

2. Define your recovery requirements

For each data class, define your recovery requirements. There are two key requirements to define:

- **Recovery Time Objective (RTO)** is the amount of time elapsed between a loss or disaster and the restoration of business operations. It is the time required to physically recover the data or application and have it ready for use. Managing the recovery time of data that is mission-critical to your business is clearly a requirement. You want your RTO to be as short as is fiscally sound for your business.
- **Recovery Point Objective (RPO)** is the point in time that recovered data will be recovered to. For example, if you recover a file that was backed up yesterday then your recovery point is one day. Managing the recovery point of data that changes very frequently is clearly a requirement as well. You want it as "close to current" as is fiscally sound for your business.

Critical questions to consider:

- How quickly do we need the data or the application restored or up and running if it is lost or corrupted?
- What is the impact of losing the most recently created data?

Again, be sure to solicit feedback from cross-functional groups outside of IT to thoroughly understand the implications of downtime and data loss.

TAILORING YOUR DATA PROTECTION SOLUTION TO THE RIGHT MIX OF STAGING AND BACKUP/ RECOVERY APPROACHES IS ACCOMPLISHED BY DEFINING THE RTO AND RPO FOR YOUR VARIOUS TYPES OF DATA BASED ON THE TRADE-OFF BETWEEN YOUR BUSINESS NEEDS AND COST.

3. Create your data protection strategy

Key considerations:

- **Backup/Recovery and Staging Tradeoff** - Tailoring your data protection solution to the right mix of staging and backup/recovery approaches is accomplished by defining the RTO and RPO for your various types of data based on the tradeoff between your business needs and cost.
- **The Case for Archiving Your Static Data**
  - First, archives provide long-term protection of data for compliance purposes.
  - Second, they make historical data available for repurposing in new applications.
  - Finally, archiving can provide performance benefits for your company. These performance benefits are realized in the following ways:
    - Once static data is moved to an archive it is no longer mixed in with your dynamic data, and therefore does not need to be backed up repeatedly. For most organizations, this means the time and storage required to complete a full backup can be reduced significantly. Plus, separating static data from your dynamic data can also significantly reduce the amount of time required to search for files.
- **Backup to Disk** - Using disk-based data protection techniques to protect your dynamic data and make disaster recovery copies will allow you to gain the most from your investment in data protection. Disk-based data protection enables faster recovery times and helps to dramatically reduce your administrative time and costs.
- **Real-Time Data Protection** technologies provide your business with the maximum RTO and RPO benefits. Best-of-breed real-time data protection solutions will allow you to recover your data back to any point in time, down to the second, and some even work to provide a high availability solution for your applications to allow for failover of the application to bring them back up within seconds.

For most medium-sized businesses the number of data classes and their related strategies might be three. For example:

Data Class	Recovery Objectives Time Point		Data Protection Strategy
Mission-Critical / Continuous Change	Less than 5 Minutes	Less than 5 Minutes	High value data that is considered mission-critical to your business will likely require a level of real-time protection, local data protection copies and the creation of disaster recovery copies.
Business-Vital / Moderate Frequency of Change	6 - 24 Hours	2 - 12 Hours	High value data that is important to your business and can be served by full/ incremental backups, disaster recovery copies, disk-based backup and rapid recovery systems.
Static / Very Low Frequency of Change Data	Less than 72 Hours	Less than 24 Hours	To be separated from dynamic data, moved to an archive, backed up once, copied and moved off-site for disaster recovery and compliance purposes

EASE OF USE IS A VERY IMPORTANT REQUIREMENT. YOU MAY RECOGNIZE THE NEED TO PROTECT YOUR DATA, BUT WITH YOUR OTHER RESPONSIBILITIES, YOU PROBABLY DON'T HAVE TIME TO BECOME A DATA PROTECTION EXPERT.

4. Select the right data protection solution to serve your business strategy

How important is the data to your business? Once you have established your data classifications and defined appropriate strategies for managing each, you can then select a set of data protection solutions that match your business requirements.

Your data protection solutions should be tailored to your business needs and provide cost-effective approaches to managing the different types of data in your environment. They should also be:

- **Easy to Implement and Manage** - Ease of use is a very important requirement. You may recognize the need to protect your data, but with your other responsibilities, you probably don't have time to become a data protection expert. Metaphorically, you want to have data protection perform as a utility. You want the lights to come on when you throw the switch, but you probably don't want to have electricians on staff. You need data protection solutions that are easy to implement and manage. Ease of use will significantly reduce the people costs of protecting data.
- **Cost-Effective** - You want to minimize the technology cost of protecting your data. The best way to do this is with a combination of storage solutions that is managed transparently to meet your business requirements at the lowest possible cost. Doing the work to identify and classify your data based on criticality and frequency of change will allow you to buy only what your business needs.
- **Secure** - You want to make sure that your data is secure and that you are protecting the privacy of your employees, customers and business partners. For instance, copies of data made for backup should maintain the same level of security that exists in your primary data systems. Often this means encrypting the data.
- **Comprehensive** - Your data protection solution should be able to automatically address the needs of all of the systems within your environment. That includes any device attached to your network. Organizations of all sizes frequently have problems with effectively protecting workstations, laptops and other mobile devices. Your solution should be able to identify mobile devices when they are attached to your network and collect the appropriate data for protection.
- **Scalable** - Consider how you expect your business to change over the next few years and be certain to include these expectations when thinking about the available data protection solutions. Adaptable and scalable solutions may be important to you if your requirements are likely to change significantly. Deduplication can enhance your ability to deal with data growth over time as well as support a cost-effective data protection strategy.

- **Designed to Support Best Practices** - Finally, you want to be confident that you are fully protected. The horror stories are in fact, true. Businesses do cease to exist as a result of inadequate data protection strategies. You need to make sure that the vendors who build your data protection solutions are specialists with deep and broad experience.

5. Implement, monitor and improve

Selecting solutions that are easy to implement and manage, cost-effective, secure, comprehensive, scalable and designed to support best practices will go a long way toward making your implementation successful. You do not have to become a data protection expert, but you should become very aware of your business needs for data protection.

6. Final Points

DATA CLASSIFICATION MUST BE A COLLECTIVE AND CROSS-DEPARTMENTAL EFFORT.

As discussed in this paper, the process of data classification is the first, and very important step in the quest to ensure sufficient levels of protection for your organization's applications and data. Data classification must be a collective and cross-departmental effort. Too often there is a disconnect between IT and those who have some interaction with the data such as business managers and the IT department. Take for example, an Exchange failure in which a very capable system administrator works on a fix with the understanding that 24 hours of downtime is acceptable to the organization. Meanwhile, the CEO calls the IT director every 20 minutes for a status update – each call containing fewer pleasantries. In this case, the understood RTO of 24 hours may have been an uneducated guess or perhaps IT simply did not take into consideration the needs of all departments who rely on Exchange. In reality, Exchange should have been classified and protected as Business-Vital or Mission-Critical. Miscommunication (or a lack of communication) such as this may lead to unfortunate ramifications for individuals as well as the organization as a whole.

Of course, even if Exchange is not "Mission-Critical" it still might give users and IT pain around the backup window, or perhaps granular mail recovery. So we need to be careful how we classify data because business criticality extends to also include user protection "pain." In this example, if the Exchange server took many hours to backup, then there are technologies that can remove the pain and deliver other benefits too. If we were to base our data protection strategy purely on the classification of that Exchange server (not mission-critical), we might use traditional backup. However, in this case traditional backup would not relieve the real pain and we'd miss the opportunity to have a better solution.

In other words, it's worth noting that beyond pure RTO and RPO requirements, there may be pain points (e.g., extremely long backup windows) associated with non-Business-Vital and non-Mission-Critical data that justify the deployment of data protection technologies that may appear to be overkill. However, at the end of the day, if the pain subsides and you find yourself with more time available to work on strategic initiatives that will contribute to your organization's bottom line, the "overkill" label may quickly fade away.

This is why we say that using a thoughtful approach to defining your data classes and their level of importance, requirements, strategies, and solutions can drive business results for you, your employees, and your customers. Data protection solutions can provide an efficient way to reduce your business risk, manage data growth, and leverage your IT investments.

- Ensure your applications are continually in operation, serving your customers, and enabling your key business operations. In the event of a disruption, you can minimize the length and severity of the disruption.
- Support your needs to comply with regulations in a cost-effective and complete manner, reducing business risk and the cost of compliance.
- Provide access to information that you can leverage into business value.

Data protection solutions have the ability to protect your investment in your business. It all depends on how you implement them. You should focus on your business needs and not on technology.

Please also check our Solutions Briefs on Static, Business-Vital and Mission-Critical data:

www.bakbone.com/solutionbriefs

whitepaper

BakBone®
The Power of Simplicity™

BakBone Global Headquarters
9540 Towne Centre Drive, Suite 100
San Diego, CA 92121
Toll Free Phone: 877-939-2663
Phone: 858-450-9009
Fax: 858-450-9929
Email: sales@bakbone.com

Asia Pacific Headquarters
Shinjuku Dai-ichi-Seimei Bldg.11th Floor
2-7-1 Nishi Shinjuku, Shinjuku-ku
Tokyo, Japan 163-0711
Phone: 81-3-5908-3511
Fax: 81-3-5908-3512
Email: sales@bakbone.co.jp

Europe Headquarters
100 Longwater Avenue
Green Park
Reading
RG2 6GP
United Kingdom
Phone: 44 (0)1189-224-800
Fax: 44 (0)1189-224-899
Email: sales_europe@bakbone.com

97419_05-10-10