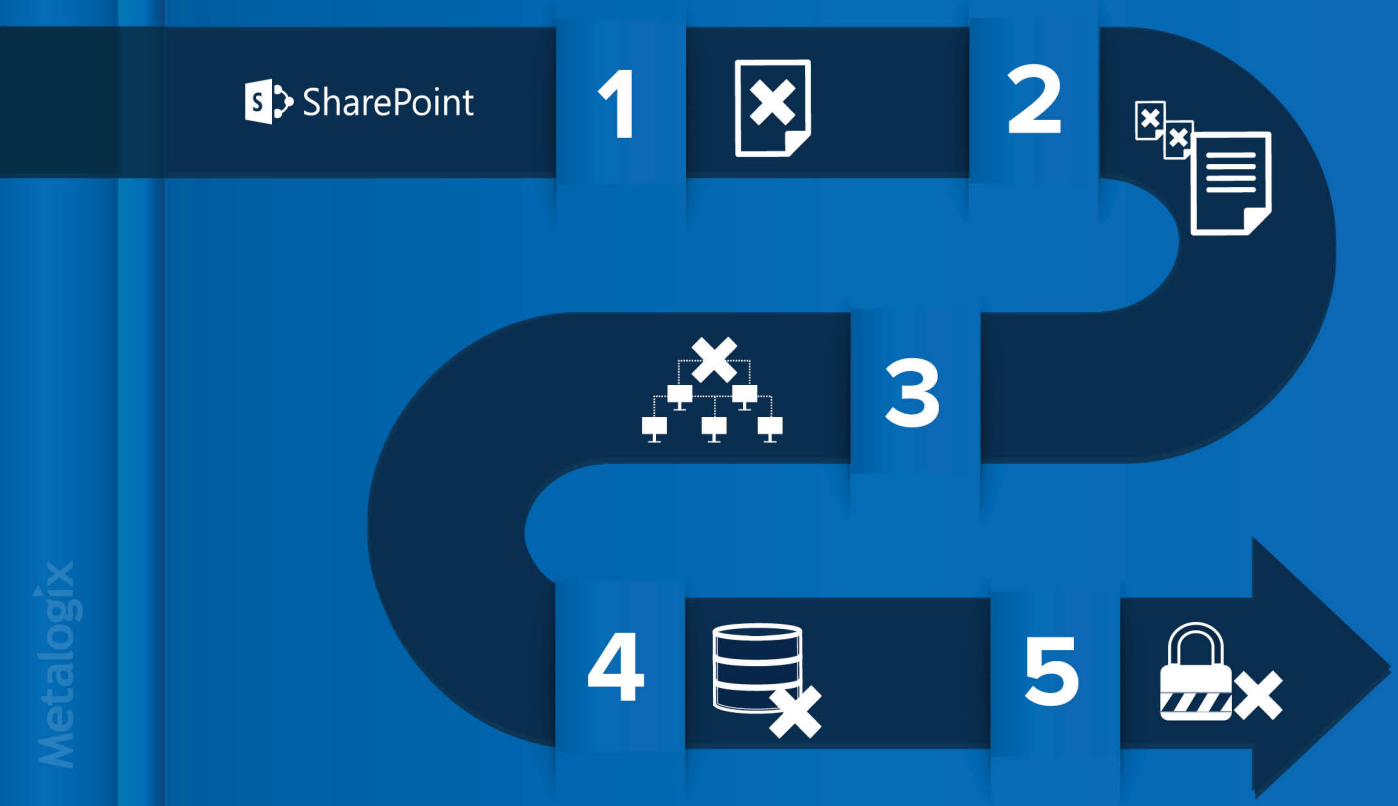
Metalogix

THE TOP FIVE

SHAREPOINT DAILY DISASTERS & HOW TO RECOVER FROM THEM

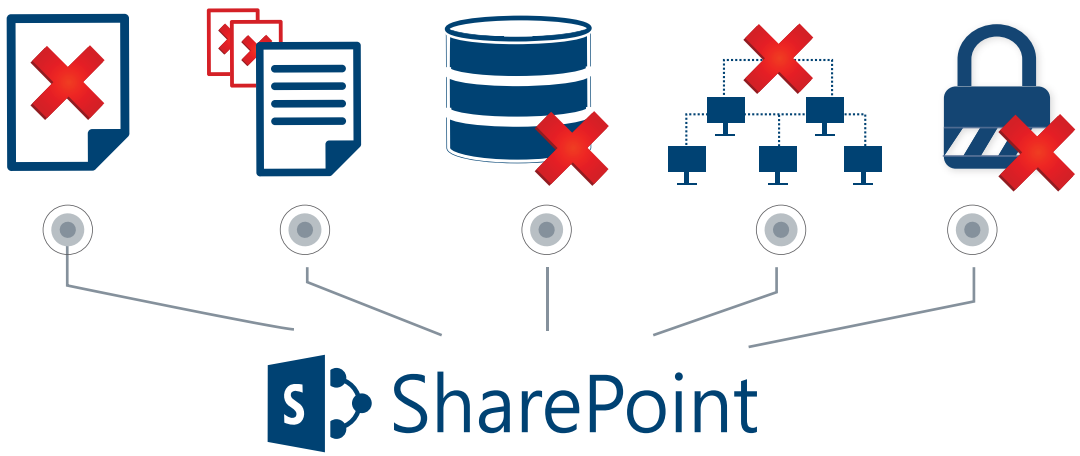


Metalogix

TABLE OF CONTENTS

INTRODUCTION

Disaster recovery is not a flashy or exciting discussion topic by many standards, but most information technology professionals recognize that disaster preparedness and business continuity planning are critical to the long-term viability of their organizations. For these reasons, most companies have some plan to continue operations in the face of floods, cyber-attack, and a host of other catastrophic disasters.



Treating disasters as an all-or-nothing proposition is particularly dangerous for many of today's applications and systems, though – especially Microsoft's SharePoint platform. SharePoint is an extremely complex application platform that comprises numerous servers, services, and components. It is rare for a SharePoint farm to fail wholesale and in catastrophic fashion, but it is not uncommon for some smaller piece or component of a SharePoint environment to fail now and then.

These "daily disasters" – minor but semi-regular failures in some aspect of a SharePoint environment – are what tend to keep administrators busy in their day-to-day jobs.

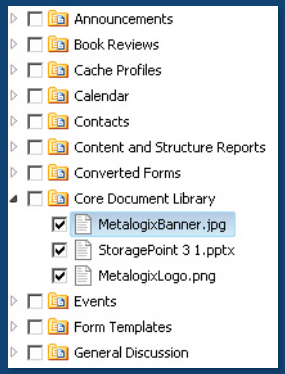
Let's take a look at some of the most common daily disasters and offer some practical steps to avoid them.

RESTORING MISSING DOCUMENTS

Administrators are frequently tasked with addressing user requests to restore missing SharePoint content. While the introduction of Recycle Bin in SharePoint 2007 went a long way to reduce these requests, they still occur.

Oftentimes, a user can retrieve documents without the assistance of an administrator, if they act quickly. However, SharePoint's Recycle Bins do not hold their contents forever. Most environments are configured to automatically flush their Recycle Bins for reasons of content size (i.e., too much in a bin) and age (i.e., a document is too old).

Documents can also disappear as a result of workflow and information management policies (such as retention policies). These may move documents between sites and site collections without a user's knowledge. In some cases, these same mechanisms may delete documents entirely.



FOLLOW THESE STEPS TO MITIGATE THE "DISAPPEARING DOCUMENT" PROBLEM:

> Ensure that both first and second stages of the SharePoint Recycle Bin are enabled. Ideally, an item-level backup and restore strategy should be implemented to ensure that documents can be recovered in the event that they "disappear."

> If you're charged with restoring a document and the above stages weren't yet enabled, you'll need to identify compositional differences between the past and present states of the target document library. This is a less than ideal solution, for anything but the smallest of document libraries, this process can be extremely tedious and time consuming at best with conventional SharePoint administrative tools.

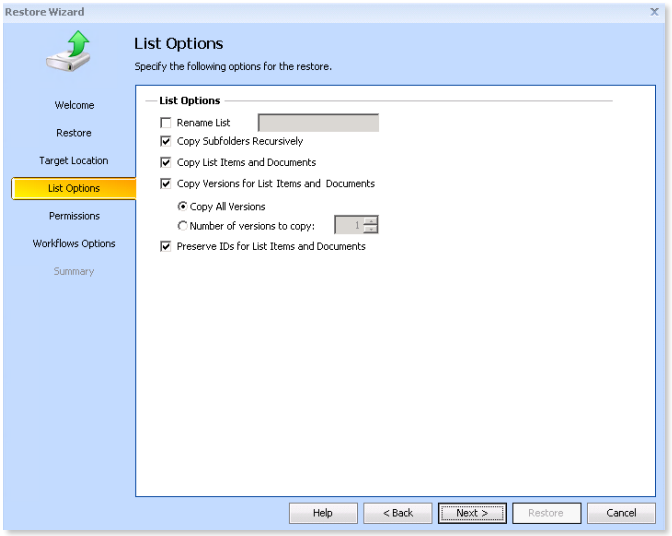
Multiple deletions from a document library is another problem. In these cases a user may not know which documents were deleted – only that they need to restore everything that went missing after at a particular time.

RESTORING PREVIOUS VERSIONS OF DOCUMENTS

DOCUMENT VERSION RECOVERY IS A COMPLEX PROCESS AND CRITICAL TO USERS. BE SURE TO ADOPT A LAYERED APPROACH TO ENSURE DOCUMENT VERSION RESTORES ARE SIMPLIFIED:

> Turn on versioning within document libraries.

> Enforce a document check-in/check-out to ensure only one user is working on a document at any given time.



Restoring documents that don't exist in the form that matches user expectations is another common problem.

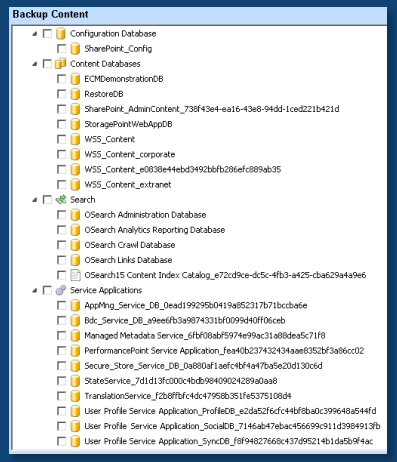
This often occurs when versioning for the list or library isn't enabled – eachtime a user saves a document back to SharePoint, that document overwrites its previous version. However, versioning isn't a fix-all solution. If you're storage-conscious and limit the number of document versions that can be retained – then a complete document history may not be available. In fact, once the number of check-ins permissible by the version retention policy is reached for a given document, SharePoint deletes older versions of that document to accommodate newer versions.

Documents deleted as a result of retention limits do not go to the SharePoint Recycle Bin – they are permanently gone.

CORRUPTION IN A CONTENT DATABASE

Content database corruption is problematic because it affects all users working with the site collections in that database. A SharePoint content database can house hundreds or even thousands of site collections. Having a content database fall out of circulation has the potential to affect most, if not all, users in a SharePoint environment.

Once a SharePoint environment is in-use, most administrators just create site collections as they are needed without giving much thought as to where those site collections go. Additional databases only get created as they are needed – typically when the "current" content database is reaching Microsoft's maximum size (which varies from 200GB to quite a bit larger depending on the performance of the underlying SQL Server).



CORRUPTED CONTENT DATABASES ARE A TRICKY PROBLEM WITH VERY FEW PRACTICAL FIXES. HERE AT METALOGIX, WE RECOMMEND YOU TAKE THE FOLLOWING STEPS TO PROTECT AGAINST SUCH SCENARIOS:

> Perform regular content database backups.

> As with all backup regimens, test frequently to ensure that you can restore as desired!

Out-of-the-box high availability (HA) mechanisms generally do little to help with corrupted content databases. Some HA mechanisms, such as SQL Server's mirroring and AlwaysOn Availability Groups, have the ability to repair inconsistencies that occur during mirroring or replication. If the source of content database corruption is external to the mirroring or replication mechanism, though, then HA simply guarantees "highly available corruption" – not a way to repair SharePoint content.

DELETED SITE COLLECTION

It's quite common for users to unintentionally delete SharePoint site collections or sub-sites.

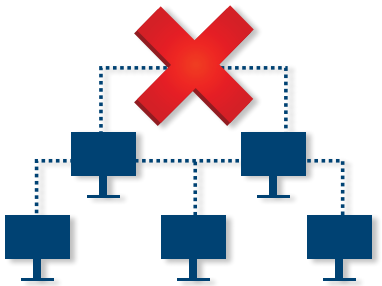
Microsoft recognized the prevalence of this problem during the SharePoint 2010 timeframe and introduced the Site Recycle Bin as part of Service Pack 1. The Site Recycle Bin extended standard Recycle Bin support to include site collections and sub-sites that were deleted. Now, although end users can restore deleted sub-sites by themselves from within the SharePoint web user interface, you'll still need to perform an administrative action to restore an entire site collection using the Site Recycle Bin.

This is due to the fact that site collections can't be restored from within the web user interface or even Central Administration. Instead, restoring a site collection for the Site Recycle Bin has to be done with PowerShell (specifically, the Get-SPDeletedSite and Restore-SPDeletedSite cmdlets) on your SharePoint member server.

LET'S RECAP. TO PREVENT AND MITIGATE THE PROBLEM OF DELETED SITE COLLECTIONS:

> Ensure that SharePoint's Recycle Bins are configured and enabled to catch deleted site collections.

> Implement a solid backup and restore strategy for site collections and/or their associated databases.



DELETED PERMISSION SETTINGS

ADMINISTRATORS CAN AVOID TIME-CONSUMING MANUAL WORK-AROUNDS WITH THE FOLLOWING STRATEGIES:

> Without the right out-of-the-box tools in place, a site collection (or content database) backup/restore is needed.

The deletion of unique permissions applied to SharePoint lists or libraries by absent-minded users is a tricky one to reverse, since SharePoint's built-in data protection toolset offers no options for restoring permissions.

The only option is to either manually re-apply all of the custom permissions to items in the list, or delete the list and attempt to import a known "good copy" that was exported from a backup set. Previously executed tests will provide much needed confidence in any restore action. The former choice is especially time consuming, while the latter results in the loss of content modifications since the last backup. Either case is far from ideal because a compromise must be made.

THE CHALLENGE WITH CONVENTIONAL PROTECTION TOOLS

A common thread that runs through the daily disasters presented herein is that they all revolve around SharePoint content. More specifically, each of the disasters involves one or more pieces of content that has changed, become corrupt, or disappeared from within a content database. This is an important fact, and it provides some indication of why conventional data protection tools fall short when it comes to recovering from a daily disaster.

CONVENTIONAL DATA TOOLS DON'T UNDERSTAND SHAREPOINT

Since conventional data protection tools don't understand SharePoint as an application and how it stores data, they are limited in how far and how deep they can go in protecting SharePoint content. In fact, most non-specific data protection tools do not understand SharePoint content beyond the depth of a content database, and so they are only able to protect SharePoint content by protecting SharePoint's SQL Server content databases.

DATABASE-LEVEL PROTECTION AND RECOVERY IS LIMITED

Unfortunately, database-level protection and recovery is insufficient for practical recovery from the bulk of the daily disasters we've outlined here because it simply is not granular enough. When SharePoint content is restored at the database level, entire site collections of data are restored at once. If you're attempting to restore just a sub-site, a document library, or some other subset of SharePoint site collection data, you're left with additional tasks such as finding target content after restore, manually exporting that content, and finding some way to merge it back into a live production environment. Although this series of recovery steps can sometimes be performed from a strictly technical perspective, they are far from ideal and acceptable when the total costs and required amount of administrative time are considered.

THE KEY TO RECOVERY

Quickly recovering from the daily disasters that stem from problems with SharePoint content requires a toolset that understands both SharePoint content and the overall application environment :

GRANUALITY

The tools understand SharePoint content at level of granularity that is deeper than the SharePoint database. As a result, these tools can work through SharePoint's exposed application programming interfaces (APIs) to more efficiently protect SharePoint content and restore only content items of interest.

BROADER FEATURE-RICH CAPABILITIES

The tools provide additional capabilities beyond basic data protection. For example, a SharePoint-specific data protection tool may provide the ability to search through backup sets for items of interest, compare current production data with backup set data to locate missing items for subsequent restore, or even provide end users with mechanisms to execute some restoration scenarios on their own.

These capabilities are important and ultimately act to reduce many of the administrative burdens commonly associated data restoration scenarios. Reducing these burdens, in turn, can result in savings – both in terms of overall data protection expenditures and RTO (recovery time objective) costs.

PREPARE FOR YOUR RECOVERY

Daily Disasters don't need to stop you in your tracks. With upfront knowledge and preparation, most daily disasters can be avoided or substantially mitigated. This eBook has provided you with actionable insights to better prepare you for several of the top SharePoint daily disaster issues you will face.

To bump up your overall level of recovery preparedness, take the next step to provide even more protection for your SharePoint environment.

SHAREPOINT RECOVERY PLANNING CHECKLIST

Download the free SharePoint Recovery Planning Checklist, an excellent resource to help you walk through the steps necessary to create an actionable recovery plan. This Recovery Planning Checklist is designed to make it easy for the you to comprehensively prepare for a successful recovery effort.

GET YOUR SHAREPOINT RECOVERY PLANNING CHECKLIST NOW AT
WWW.METALOGIX.COM/RESOURCES/PROMOTIONS/REPLICATOR/WHITE-PAPERS-AND-E-BOOKS/SHAREPOINT-RECOVERY-PLANNING-CHECKLIST.ASPX

THE CHECKLIST ORGANIZES THE INFORMATION YOU NEED TO BE AWARE OF, INCLUDING:

- ✓ *Understanding the key recovery planning issues*
- ✓ *Analyzing your specific environment, content, outage history, and support*
- ✓ *Defining a plan, including RTO, RPO, SLA and scenario events*
- ✓ *Securing organizational and executive support*
- ✓ *Testing the plan to validate and provide peace of mind*
- ✓ *Revision assessment and execution*