

# SHAREPOINT

PRACTICAL IT STRATEGIES FOR ENTERPRISE COLLABORATION /// JUNE 2009

M

## MANAGEMENT

### **Managing Documents By Content Type**

*SharePoint falls short when it comes to classifying documents.  
Learn some useful approaches that can help accomplish the task.*

BY BRIEN M. POSEY

I

## IMPLEMENTATION

### **Strategies for Securing SharePoint in Windows**

*Plan for security at the start of your SharePoint deployment  
to control access, applications and content.* BY STEPHEN CUMMINS

G

## GOVERNANCE

### **Four Big SharePoint Governance Mistakes**

*Steer clear of problems by taking some simple steps  
in your governance process.* BY PAUL WEST

# Easy Fixes for SharePoint Woes

BY CHRISTINE CASATELLI

## Editor's Note

M

**Managing Documents by Content Type**

I

**Strategies for Securing SharePoint in Windows**

G

**Four Big SharePoint Governance Mistakes**

**IF YOU HAVEN'T** figured it out yet, SharePoint isn't perfect—especially when it comes to classification. Even though SharePoint was created as a content management platform, it lacks an easy way to categorize documents.

Not to worry. Microsoft MVP Brien M. Posey has devised some alternate approaches to get the job done. In "[Managing Documents by Content Type](#)," Posey walks you through the process of defining new content types so that you can archive or delete project-related documents, for example, in no time.

When it comes to SharePoint security, planning is key. It's best to focus on access control, application security and content security. Read "[Strategies for Securing SharePoint in Windows](#)" by SharePoint MVP Stephen Cummins for some tips on how to keep your installation safe. Cummins says not to retrofit security onto a SharePoint site. Creating clear policies at the start will ensure that SharePoint remains as secure as possible.

Governance got you down? Are you paying too much attention to deleting files that don't belong on the portal and not enough to fixing the processes that allowed them to be there? SharePoint guru Paul West can help you navigate the minefield in "[Four Big SharePoint Governance Mistakes](#)." West describes the most common SharePoint gaffes when it comes to site governance and how to avoid them. Don't say we didn't warn you.

What was your biggest SharePoint mistake? How did you fix it? I want to hear all about it. Send me an email at [ccasatelli@techtarget.com](mailto:ccasatelli@techtarget.com). ■



SearchWinIT.com

©2009 TECHTARGET.  
ALL RIGHTS RESERVED.

Cathleen Gagne, Editorial Director, [cgagne@techtarget.com](mailto:cgagne@techtarget.com)

Christine Casatelli, Editor, [ccasatelli@techtarget.com](mailto:ccasatelli@techtarget.com)

Martha Moore, Copy Editor, [mmoore@techtarget.com](mailto:mmoore@techtarget.com)

Linda Koury, Art Director of Digital Content, [lkoury@techtarget.com](mailto:lkoury@techtarget.com)

Jonathan Brown, Publisher, [jebrown@techtarget.com](mailto:jebrown@techtarget.com)

Peter Larkin, Senior Director of Sales, [plarkin@techtarget.com](mailto:plarkin@techtarget.com)

TechTarget, 117 Kendrick Street, Needham, MA 02494; [www.techtarget.com](http://www.techtarget.com)

# Managing Documents By Content Type

Editor's Note

M

Managing  
Documents by  
Content Type

I

Strategies  
for Securing  
SharePoint  
in Windows

G

Four Big  
SharePoint  
Governance  
Mistakes

*SharePoint falls short when it comes to classifying documents.  
Learn some useful approaches that can help accomplish the task.*

BY BRIEN M. POSEY

**ALTHOUGH MICROSOFT OFFICE** SharePoint Server 2007 is designed to be a content management product, it is lacking in some areas. But there are ways SharePoint administrators can work around the deficiencies.

One area where SharePoint falls short is classification. Microsoft doesn't really offer a good way to categorize documents in SharePoint. To understand why this is important, imagine that you have a collection of documents that are all related to a specific project. It would be really nice to be able to classify those documents as being connected with the project. That way when the project is completed, all of the documents that are related to the project could be archived or deleted.

Another benefit to being able to classify documents in this way is that if someone new joins the team who is responsible for the project, it would

be easy to assign that person rights to all of the documents that are related to the project.

Although SharePoint does not allow SharePoint administrators to classify documents in this way at the schema level, there are a few different approaches that will do the job. Probably the easiest option would be to create a dedicated document library specifically for the project. This isn't always practical, though, because corporate policies or regulatory issues may prevent it.

A brief explanation: Although there aren't any regulatory issues that specifically prevent you from creating a document library, there are plenty of regulations that dictate how the data must be managed. It's important to keep in mind that creating a project-oriented document library may lead to regulatory violations because of lack of planning and oversight.

Editor's Note

M

Managing  
Documents by  
Content Type

I

Strategies  
for Securing  
SharePoint  
in Windows

G

Four Big  
SharePoint  
Governance  
Mistakes

Another option is to define content types within a document library. Content types are primarily designed to allow metadata to be linked to documents based on document type. For instance, you might consider using one set of metadata fields for news releases and another set of metadata

fields for invoices.

Although content type is primarily designed to differentiate between types of documents, you can use it for other purposes. You could create a content type for your particular project, and then tell everyone who is involved in the project to use only

## Defining a New Content Type

IT'S IMPORTANT TO note that SharePoint does not create any content types by default. In previous versions of SharePoint, you had two choices:

1. Make populating the metadata fields optional. That way, you could fill in only the fields that apply to a specific document.
2. Create separate document libraries for each type of document.

In Microsoft Office SharePoint Server 2007, however, administrators can define a new content type and apply it to documents. To create a new content type, click the Site Actions button, select Site Settings, and the option command Modify All Site Settings. Next, click the Site Content Types link located in the Galleries section on the following page. Now click the Create button. You'll be directed to the "New Site Content Type" page where you'll have to fill in a few simple fields.

You can include a newly created content type in a document library by going to the "Site Settings" page and clicking the Site Libraries and the Lists links found in the Site Administration section.

Next, click the link to customize your document library. The "Customize Documents" page contains a Content Type section. If you click the Add From Existing Site Content Types link, you will be given the chance to add stock or custom content types to the document library.

It's fairly easy to define a new content type in SharePoint. And when you click on an individual content type, it allows you to specify metadata for that content type. —SEARCHWINIT.COM

## » MANAGEMENT

that specific content type when creating project-related documents. Although this approach isn't completely ideal, it gives you the option of creating expiration policies that are content type-specific.

To set an expiration policy that is based on content type, open your SharePoint document library and choose the Document Library Set-

tings command from the document library's Settings menu—not the Site Actions menu. When you do, SharePoint will open the Customize Documents page. Scroll through this page until you find the Content Types section, as shown in **FIGURE 1**.

As you can see in **FIGURE 1**, the Content Types section lists all of the content types that have been defined so

Editor's Note

M

Managing Documents by Content Type

I

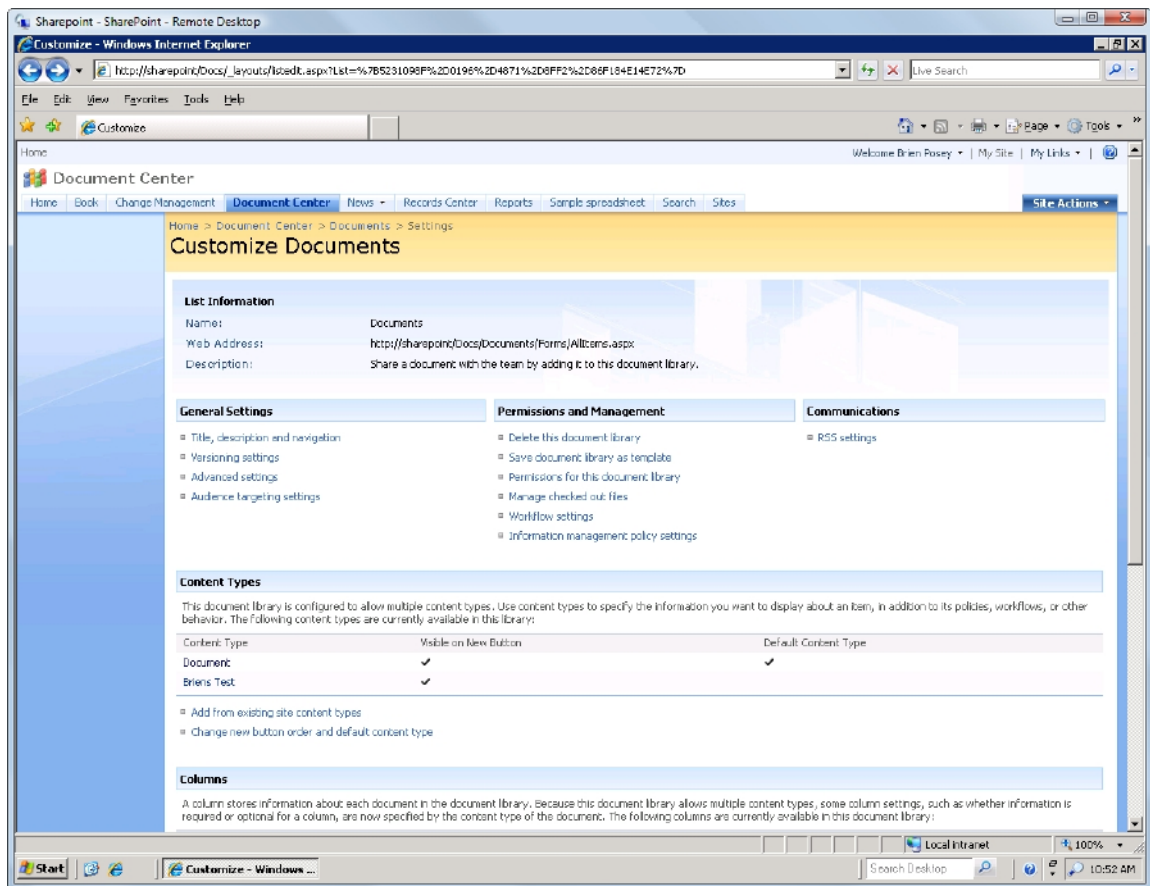
Strategies for Securing SharePoint in Windows

G

Four Big SharePoint Governance Mistakes

FIGURE 1

*The Content Types section lists all of the content types that have been defined.*



## » MANAGEMENT

far. Click on the content type that you want to set the expiration policy on, and then click the Information Management Policy Settings link located on the following page.

The Information Management Policy Settings page allows you to either define a new policy or to reuse a previously defined policy. Because we are trying to create a unique expira-

tion policy that's based on content type, click the Define a Policy radio button, and then click OK.

You will now be taken to the Edit Policy page. I recommend starting out by entering a description and a policy statement for the policy that you are creating. When you are done, select the Enable Expiration check box, as shown in **FIGURE 2**.

### Editor's Note

#### M

Managing Documents by Content Type

#### I

Strategies for Securing SharePoint in Windows

#### G

Four Big SharePoint Governance Mistakes

FIGURE 2

Select the Enable Expiration check box.

Sharepoint - SharePoint - Remote Desktop

Edit Policy - Windows Internet Explorer

http://sharepoint/docs/\_layouts/policyconfig.aspx?List=%7b5231098f-0196-4871-8ff2-36f164e14e72%7d&type=0x010100A39E5B62CF1D64D9FB2...

Edit Policy

### Edit Policy: Document

**Name and Administrative Description**  
The name and administrative description are shown to list managers when configuring policies on a list or content type.

Name:

Administrative Description:

**Policy Statement**  
The policy statement is displayed to end users when they open items subject to this policy. The policy statement can explain which policies apply to the content or indicate any special handling or information that users need to be aware of.

Policy Statement:

**Labels**  
You can add a label to a document to ensure that important information about the document is included when it is printed. To specify the label, type the text you want to use in the "Label format" box. You can use any combination of fixed text or document properties, except calculated or built-in properties such as GUID or CreatedBy. To start a new line, use the \n character sequence.

☐ Enable Labels

**Auditing**  
Specify the events that should be audited for documents and items subject to this policy.

☐ Enable Auditing

**Expiration**  
Schedule content disposition by specifying its retention period and the action to take when it reaches its expiration date.

☒ Enable Expiration

The retention period is:  
☐ A time period based on the item's properties:  
Created +  years  
☐ Set programmatically (for example, by a workflow)

When the item expires:  
☐ Perform this action:  
Delete  
☐ Start this workflow:  
Collect Signatures

---

## » MANAGEMENT

---

### Editor's Note

M

**Managing Documents by Content Type**

I

**Strategies for Securing SharePoint in Windows**

G

**Four Big SharePoint Governance Mistakes**

Upon doing so, the Expiration section will expand to show the various expiration-related options that are available. The first thing that you need to do is define a retention period. Typically, you would set the retention period based on the most recent date that the document was modified, but you can also set the retention period programmatically based on workflows.

After you have defined the retention period, you must specify what happens when the retention period expires. You have the option of deleting the document, deleting the record and submission information or launching a work flow. When you are done, click OK, and the policy will be set.

Although SharePoint does have some nice document management features, it isn't perfect. Defining new content types is not an ideal solution for classifying documents in Share-

Point, but for now it's the best method available without purchasing

*Defining new content types is not an ideal solution for classifying documents in SharePoint, but for now it's the best method that is available without purchasing third-party add-ons or developing an add-on yourself.*

third-party add-ons or developing an add-on yourself. Hopefully Microsoft will give SharePoint administrators a better way of classifying documents in the next version. ■

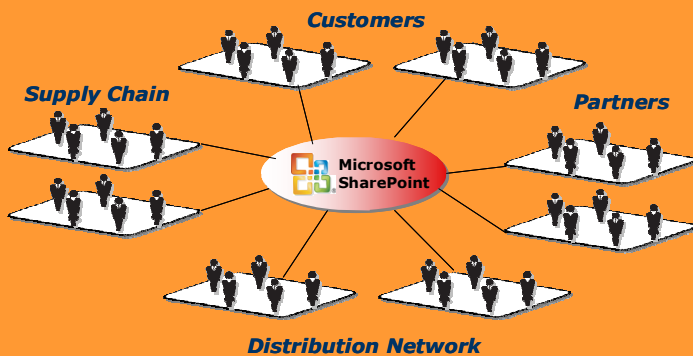


### ABOUT THE AUTHOR

**Brien M. Posey** has received Microsoft's Most Valuable Professional award five times for his work with Windows Server, IIS, file systems/storage, and Exchange Server. He has served as CIO for a nationwide chain of hospitals and healthcare facilities and was once a network administrator for Fort Knox.



# Is Your SharePoint Deployment Ready for Extranet Use?



***Over 70% of enterprise businesses plan to extend SharePoint to extranet users\*, yet few are prepared to support it***

\* Source: 2008 Epok survey

## Secure SharePoint Extranets Epok Edition for Microsoft® SharePoint

Epok products and consulting services let you seamlessly extend SharePoint to external partners and customers to increase business agility, improve security and simplify IT operations.

### Security and Compliance

- Integrate business agreements with every user activity
- Consolidate auditing across site collections and farms
- Watermark sensitive documents

### Ease of Provisioning

- Empower site owners to manage extranet users and access rights
- Delegate user management to external partners

### Enterprise Scale

- Group definition and site discovery span site collections and farms
- Integrate existing security infrastructure: ISA/IAG, 2-Factor authentication and CAC cards
- Fill FBA gaps: MySites, MS Office client integration

**Register for a free webinar on planning for SharePoint extranets:**  
[www.epok.net/webinar\\_list.html](http://www.epok.net/webinar_list.html)



# Strategies for Securing SharePoint in Windows

Editor's Note

M

Managing Documents by Content Type

I

Strategies for Securing SharePoint in Windows

G

Four Big SharePoint Governance Mistakes

*Plan for security at the start of your SharePoint deployment to control access, applications and content.* **BY STEPHEN CUMMINS**

**WHEN IT COMES** to securing SharePoint Server, decisions are best made during the planning stages of SharePoint deployment because it's difficult to retroactively apply security policies. When formulating security strategies, focus on three key areas: access control, application security and content security.

## PRACTICAL COMPROMISE THROUGH ACCESS CONTROL

The main way to secure SharePoint is through access control. SharePoint allows users to create and manage their own groups, but there are ways to control them. The IT department can create Active Directory roles within SharePoint groups so only those authorized to use AD management tools can grant and change access permissions.

Centralized access management leads to greater control and more effi-

ciency, but it also slows down users when they are creating their own structures and granting access to them. A practical compromise is to control access to top-level department sites and enterprise-wide sites

*The IT department can create Active Directory roles within SharePoint groups so only those authorized to use AD management tools can grant and change access permissions.*

from Active Directory and IT but to have areas in SharePoint where users can create ad hoc sites and grant access to them themselves.

These areas would then be man-

## » IMPLEMENTATION

aged using policies and quotas. For example, if a SharePoint site is not accessed for 90 days, the administrator would be asked whether to keep it or delete it. Those sites can also have size limits where administrators would be notified by email if they reach 80% of capacity. With that, no more content could be added when they reach 100%.

### PROTECT PERFORMANCE WITH APPLICATION SECURITY

Application security policies protect against denial-of-service attacks and anything that might compromise the performance or stability of the SharePoint Server platform. For the first layer of protection, apply the principles of least privilege during installation to the service accounts SharePoint uses to run the application.

To complete this process, follow the steps outlined in [TechNet's Plan for administrative and service accounts \(Office SharePoint Server\)](#), which provides requirements and recommendations for configuring administrative and service accounts.

One thing to remember is that SharePoint Server can be added to and customized because it is, at its core, an ASP.NET application. There are many ways code or markup changes can interfere with the system. Clear policies at the start will ensure that SharePoint remains as

secure as possible.

Once again, apply the principles of least privilege here. Custom code needs execute permission to run, and this is a high-level privilege. Here are three ways to provide this level:

**1. You could edit the virtual server's web.config file from minimal to medium or full.** This is not recommended because it allows too much latitude to the code.

**2. You can install the assemblies in the GAC, or global assembly cache.** This provides very high privileges, but there is no way to control what the code can do and what it cannot do.

*Application security policies protect against denial-of-service attacks and anything that might compromise the performance or stability of the SharePoint Server platform.*

The solution is custom policy files, which are difficult to implement but are the most secure way to deploy assemblies. To learn more about code

Editor's Note

M

Managing Documents by Content Type

I

Strategies for Securing SharePoint in Windows

G

Four Big SharePoint Governance Mistakes

---

## » IMPLEMENTATION

---

access security, review [Microsoft Windows SharePoint Services and Code Access Security](#).

**3. You can use SharePoint Designer, which is a free productivity tool that has many benefits,** but it can create security headaches because sites can become inaccessible. It can, however, be locked down at a number of levels by removing specific permissions within SharePoint.

### POLICIES GUIDE CONTENT SECURITY

Securing SharePoint's content requires policies that dictate how, where and who can publish and share content and for what audience. For example, some companies may restrict employees from having blogs to control how they share sensitive information with the public.

Although policy restrictions may

make it clear to employees that unauthorized sharing is prohibited, you may want to be more proactive by creating channels that do allow information to be shared but in a way that means it is vetted and approved first. To create channels that restrict viewing before content is approved, use approval workflows.

It's important to note that even though "audiences" can be defined to target what content can be viewed, they do not secure it. Anyone can still access information as long as he or she has the appropriate access rights.

Business conditions and circumstances change all the time, so security policies must be reviewed and improved regularly to keep in step with business needs. SharePoint allows users and developers to be in control. They need clear rules that allow maximum freedom and maintain security, stability and—most important—performance. ■

#### Editor's Note

M

[Managing Documents by Content Type](#)

I

[Strategies for Securing SharePoint in Windows](#)

G

[Four Big SharePoint Governance Mistakes](#)



#### ABOUT THE AUTHOR

**Stephen Cummins** is founder of [www.spsfaq.com](http://www.spsfaq.com) and a SharePoint consultant. Cummins has been a SharePoint Most Valuable Professional for the past seven years. He lives in Kildare, Ireland, with his wife, daughter, two dogs and an ever-changing number of goldfish. Cummins is a globally known expert with experience delivering Microsoft enterprise technology into complex environments. His core technologies are SharePoint Server, Windows SharePoint Services, Search Server, IIS, SQL Server, Windows Server, Office, InfoPath and Microsoft Project Server.



**Don't Get Caught  
With Your  
Pants Down...**

**AvePoint's Got  
You Covered!**

**FREE DOWNLOAD at  
[www.AvePoint.com](http://www.AvePoint.com)**

***Complete Backend  
Management for  
SharePoint***

**FREE module  
for item-level  
restores from  
SQL backups ...  
Yes, yours FREE!**

**SharePoint Backup and Recovery, Administration, Replication,  
Archiving, Compliance, eDiscovery, Reporting, and Migration**

# Four Big SharePoint Governance Mistakes

Editor's Note

*Steer clear of problems by taking some simple steps in your governance process.* BY PAUL WEST

M

Managing Documents by Content Type

I

Strategies for Securing SharePoint in Windows

G

Four Big SharePoint Governance Mistakes

**THE MICROSOFT SHAREPOINT** platform makes it easy for organizations large and small to develop shared portals, allowing for greater collaboration and improved workflow management for teams working across the building or across the country.

Unfortunately, “easy to develop” doesn’t mean that they’re easy to maintain. Even the most well meaning administrators can get into trouble when trying to maintain governance over a SharePoint site.

Here are two of the biggest SharePoint governance mistakes along with the steps you should take to avoid trouble:

■ **Taking on too much at the beginning.** When new SharePoint administrators begin governance duties on a shared portal, they see all of the wonderful functionality the platform offers, including advanced workflows and business intelligence. They want

to turn on all the bells and whistles. This makes the learning curve very steep for users and administrators alike.

End users may have more difficulty adapting to the new collaborative way of working. They may shun the portal if they find it too confusing and if they are presented with too many options at once.

Administrators can find that they have trouble problem-solving—specifically, not being able to track a problem to its source. If there are too many possibilities, then it’s hard to pinpoint which bell or whistle is causing the issue.

Rolling out SharePoint functionality in stages is a much better way to begin a portal. Start with the basic out-of-the-box collaboration and then move on to more features such as custom lists and workflows once users and administrators have gotten used to the system.



**Editor's Note****M****Managing Documents by Content Type****I****Strategies for Securing SharePoint in Windows****G****Four Big SharePoint Governance Mistakes**

■ **Duplicating too much information.** Every department or team wants its own information in its own folders. But much of the shared work on the SharePoint portal is there because it belongs to the organization as a whole. Duplicating files and documents can quickly defeat the purpose of a shared portal.

To avoid duplication, take inventory of the information that will be stored on the portal and conduct regular updates of that information. Keep track of the key information for each department as well as the information that is needed by everyone to ensure that all users get what they need from the system. Honing in on which content types are relevant for which user groups will help this process.

Once administrators realize there is trouble with their collaborative portal, more often than not, they make things worse by trying to fix the situation. Here are two big blunders that administrators make while trying to clean up and some tips for avoiding them:

■ **Examining data and ignoring processes.** Too many administrators look for trouble with the data on the portal without examining the processes that lead to the data being there. A good administrator establishes processes to keep the “junk” out.

If the administrator discovers that the team is always storing personal files on the portal, then he or she needs to step in with clearly defined parameters about what belongs and what doesn't. Depending on company policy, setting your portal to block files such as MP3s can also keep the wrong content out.

Storing old data can lead to trouble as well. Sites become overcrowded and much less useful if they aren't constantly being trimmed. Administrators can set up regular archiving for items older than a set amount of time. To prevent a lot of headaches, create site and document-archiving strategies and processes for items that have lost their relevance or are no longer active.




















■ **Looking at the site through tired eyes.** When trying to fix a portal that has grown out of control, it can be easy to forget what the original intent was. When trying to fix what went wrong, it is best to step away from the situation, perhaps over a weekend, and come back to the situation with fresh eyes.

It's also a good idea to bring in someone who isn't as close to the project as the administrator is to offer perspective. This could be one of the users in the organization, someone from the governance committee who is not involved with the portal on a

*(Continued on page 16)*

## Using SharePoint Usage Reports

DATA FOR THE reports generated by Microsoft Office SharePoint Designer 2007 is saved on the server on which the site is hosted. Server administrators can grant or deny access to these reports. To run usage reports, you must have the View Usage Data permission, and the server administrator must turn on usage data collection on the server. By default, usage data collection on the server is turned off. A Site Summary report provides a high-level overview of your site, as well as links to more detailed reports listed below:

Web Site			
Site Summary ▼			
Name	Count	Size	Description
 <a href="#">Usage data</a>	660	22202KB	Hits and download bytes for the current Web site
 <a href="#">All files</a>	111	731KB	All files in the current Web site
 <a href="#">Pictures</a>	15	234KB	Picture files in the current Web site
 <a href="#">Unlinked files</a>	645	22168KB	Files in the current Web site that are not linked to any page
 <a href="#">Linked files</a>	10	5870KB	Files in the current Web site that are linked to any page
 <a href="#">Slow pages</a>	20	6870KB	Pages in the current Web site that load slowly
 <a href="#">Older files</a>	160	8202KB	Files in the current Web site that are older than 30 days
 <a href="#">Recently added files</a>	10	4870KB	Files in the current Web site that were added in the last 30 days
 <a href="#">Checked out files</a>	4235	2KB	Files in Web site that are checked out
 <a href="#">Hyperlinks</a>	161		All hyperlinks in the current Web site
 <a href="#">Unverified hyperlinks</a>	20		Hyperlinks pointing to unverified sites
 <a href="#">Broken hyperlinks</a>	1161		Hyperlinks pointing to unavailable files
 <a href="#">External hyperlinks</a>	3074		Hyperlinks pointing to files on other servers
 <a href="#">Internal hyperlinks</a>	0		Hyperlinks pointing to other files in the current Web site
 <a href="#">Component errors</a>	0		Files in the current Web site that have caused errors
 <a href="#">Style Sheet Links</a>	20		All Style Sheet Links in the current Web site
 <a href="#">Dynamic Web Templates</a>	3		All files that are associated with Dynamic Web Templates
 <a href="#">Master Pages</a>	647		All files that are associated with Master Pages
 <a href="#">Customized pages</a>	643	16150KB	Files from the SharePoint site that have been customized

SOURCE: MICROSOFT

Editor's Note

M

Managing Documents by Content Type

I

Strategies for Securing SharePoint in Windows

G

Four Big SharePoint Governance Mistakes



---

## » GOVERNANCE

---

### Editor's Note

M

**Managing Documents by Content Type**

I

**Strategies for Securing SharePoint in Windows**

G

**Four Big SharePoint Governance Mistakes**

(Continued from page 14)  
day-to-day basis or even an outside consultant. Whether the perspective comes from elsewhere in the organization or from outside, be sure to treat “the fix” like a new implementation.

Use the opportunity to reexamine what the original driver behind implementation was and what steps might be taken to get back on track. Make the most out of the second chance.

Rather than just cleaning up messes, take the time to reorganize the whole system. Some good questions to ask are: What are teams finding useful? Is the navigation clear enough for new users?

SharePoint’s built-in usage reports (See page 15) can help administrators see what users are gravitating toward and what areas they’re ignoring. Try using Site Use Confirmation and Deletion to stay current on Site Collections that have been orphaned.

As with many helpful technology tools, SharePoint portals are only as functional as their users and administrators make them. It’s easy to let small governance mistakes turn into

*SharePoint’s built-in usage reports can help administrators see what users are gravitating toward and what areas they’re ignoring.*

major headaches. Don’t let the fixes turn them into even bigger problems. With careful thought, planning and maintenance, a collaborative portal can help teams across an organizational structure work together more closely and productively. ■



### ABOUT THE AUTHOR

**Paul West** is a co-owner and co-founder of SharePoint360 LLC, a SharePoint consulting and hosting provider. West has extensive experience with SharePoint architecture and implementations. He has been working with SharePoint technologies since the Microsoft SharePoint release in 2001.

---

## » FROM OUR SPONSOR

---



- ▶ [Epok Edition for Microsoft SharePoint](#)
- ▶ [SharePoint Extranet Solutions and Case Studies](#)
- ▶ [Free SharePoint Extranet Webinars](#)

**About Epok:** Epok provides products and services to build SharePoint solutions that meet rigorous security, scalability and extensibility requirements. Our flagship product, the Epok Edition for Microsoft SharePoint, extends SharePoint to the extranet by simplifying external user administration, improving security and boosting information compliance. Epok's experience, gained as pioneers of SharePoint extranets, gives us a unique ability to build secure SharePoint solutions that meet our client's current and future enterprise needs. Epok is a Certified Microsoft Partner with customers in a wide range of markets including healthcare, legal services, financial services, manufacturing, energy, consulting, non-profits and government agencies.

---

» FROM OUR SPONSOR

+++++



- ▶ **Introducing FREE Item-Level Restores from SQL Server backups. Download Now!**
- ▶ **SharePoint Backup, Administration, Compliance, Reporting, and Migration**
- ▶ **Have Website, Will Travel: Move your HTTP Web Content to SharePoint with Ease!**

**About AvePoint:** AvePoint is proud to be a U.S. based technology company and software innovator. Since 2001, AvePoint has been a global leader in enterprise-strength infrastructure management solutions for all Microsoft SharePoint Products and Technologies. Propelled by one of the world's largest SharePoint-exclusive development teams outside of Microsoft, AvePoint's award-winning DocAve Software Platform delivers comprehensive and flexible infrastructure support for backup and recovery, replication, migration, administration, archiving, deployment management, and compliance.