

EFFECTIVE SHAREPOINT MANAGEMENT SAVES RESOURCES, TIME, AND ULTIMATELY, MONEY!

The evolution of SharePoint seen over the last near decade has been rooted in years of studies and engineering efforts with partnerships, early adopters, Fortune 500 companies and many others. From the initial 2001 introduction, Microsoft's primary goal for SharePoint has been to broaden the empowerment of users and lessen their reliance on the traditional IT personnel for everyday task support and communications. The underlying equation used in SharePoint is simple and has proven successful. Empowered users equal improved workflows, greater information sharing, and reliable decision making – all of which turns into clear elevations in prosperity.

Despite the many benefits, companies have quickly realized the increase in user empowerment also turned a drastic increase in SharePoint management. This growth empowerment has been at the sacrifice of control and awareness of the environment itself. Some of the key contributing factors to this include:

- **Permissions Inheritance:** SharePoint doesn't have a means to collectively see the variations in permission inheritance at the site collection, site, list/library, and item levels.
- **Permission Levels:** Especially with the 2007 iterations of SharePoint, there's no clear way to track the variations in permission levels that can exist with sites that have unique permissions.
- **Centralized Reporting:** Natively, there's not for manager to obtain a "birds-eye-view" of the environment. Simply collecting a tally on all sites in the environment can be a burdensome task.

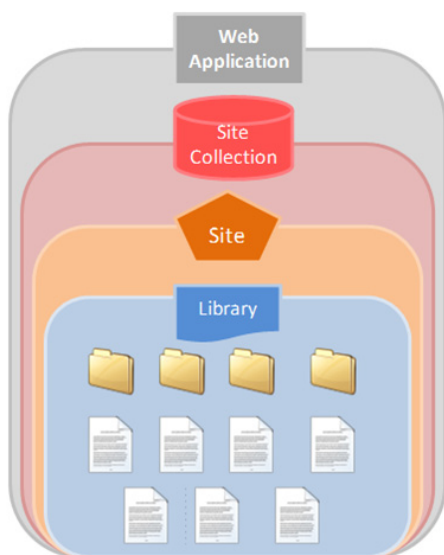
Although at first glance these factors seem nominal, they have continually proven difficult to manage. This is primarily due to the multiple management pages that naturally occur within SharePoint. Take for example a reasonable sized farm consisting of 20 site collections with a total of 1000 sub-sites, 200 of which have unique permissions. Using such a scenario, an administrator needing to conduct a simple task as discovering where a user has site permissions would require them to visit 220 different management pages. Now add some probabilities and costs to this scenario as done below:

SharePoint User Permissions Discovery	Summary
- Probability per day	25%
- Discovery Time (hours per person requested at site collection and unique sites only)	1
- Average time per day	1
- Weekly Average Time (hours)	5
- IT\SharePoint farm administrator cost (per hour)	\$60
- Yearly total cost	\$21,900.00
- Current value calculated over 3 year(s)	\$66,359.19

This and many other similar scenarios are unavoidable for any SharePoint environment. Leaving items such as inheritance, permission levels, and other factors unchecked can quickly evolve into some debilitating consequences that sneak up on management teams.

Information security is one of the biggest reasons to keep tabs on these factors. The successful increase in user empowerment seen with SharePoint has also led to an increase in the need to control sensitive materials. More and more companies find themselves liable to track who is accessing what information, what level of access is provided, and where else can they go with that access. As a small reminder, SharePoint actually opens four primary roads of access, but there's ten different ways those roads can be traveled:

Direct Permissions	SharePoint Group Membership	Site Collection Administration	Web Application Policy
<ul style="list-style-type: none"> - AD User directly assigned to an option - User is a member of an AD Group directly assigned to an object - User is a member of an AD group that is a child of a parent AD group directly assigned to an object 	<ul style="list-style-type: none"> - AD User with SharePoint Group membership assigned to an object - User is a member of an AD Group with SharePoint Group Membership assigned to an object - User is a member of an AD Group that is a child of a parent AD group with SharePoint Group membership assigned to an object 	<ul style="list-style-type: none"> - AD user/group is directly provided Site Collection Administration rights 	<ul style="list-style-type: none"> - User is assigned to a Web Application policy - User is a member of an AD group that has been provided a Web Application policy - User is a member of an AD Group that is a child of a parent AD group that has been provided a Web Application policy



Now when a manager couples these 10 scenarios with the infinite possibilities of access points at the web application – site collection, site, list/library, and item levels each with a different management page – it makes maintaining the sensitivity of information near impossible. When one adds the complexities of compliance standards such as FISMA (Federal Information Security Management Act), HIPPA mandates, and even the general legalities of running businesses today, answering the question “who has access to what?” becomes even more critical.

Security isn't the only point of contention that results from an unmanaged SharePoint environment. The following factors can easily blossom into issues for administrators as well:

- Out of control taxonomy: Not keeping tabs of who can create sites and where permissions are being assigned can lead to an excessive number of sites. This not only moves the environment away from the company's original goal or purpose, it can create a situation where storage can be of concern as well as the potential for misuse of the system.

- **Time consumption:** The manpower and resources used to locate and troubleshoot permissions, lost files are not only packing a negative impact on management teams, but come with a price tag as well.
- **Deleted Data:** Not controlling where permissions are assigned or permission level standardizations can result in situations of deleted data, sites, and loss of manpower during the look up and recovery.
- **Excessive storage:** A lack of centralized reporting often leaves management teams in limbo as far as knowing the simple number of sites and size of the environment. This leads to situations where there are overloaded site collections or content databases.
- **Duplicated Data:** Duplicated sites, lists, and documents not only increases security implications, they also increase storage demands.
- **Decreased Performance:** No maintenance or control decreases the systems effectiveness.

Remember, SharePoint as a company information sharing solution can and does elevate profits. However, to keep these benefits out-weighting the potential costs and implications associated with running SharePoint, you have to manage SharePoint. Completely understanding how SharePoint security works is the first step to effectively managing ANY environment.

1. Know how SharePoint enables individual's access to sites, lists, and libraries.
2. Know because of permission inheritance, permissions can be different at the site, list, and item levels.
3. Centralize this knowledge for the team.

Take control of these steps and guarantee that your SharePoint environment will continue to show substantial profits and benefit for your entire company.

HOW CAN IDERA HELP?

Idera SharePoint enterprise manager simplifies SharePoint administrative complexity with a series of easy to use and powerful features. From a centralized management console, take complete charge of account, site, list and item administration in SharePoint using real-time environment analytics and security reporting. Reduce the time spent on SharePoint administration while maintaining policy and compliance standards farm-wide. Come see how enterprise manager's full permissions management and auditing can help solidify the bottom-line benefits of your SharePoint environment. [Try SharePoint enterprise manager for free for 14 days here.](#)

ABOUT THE AUTHOR Since 2002, Jennifer Branham has worked as a SharePoint portal consultant providing multiple firms with planning, designing, and deployment expertise for SharePoint environments. Her SharePoint expertise includes both commercial and government SharePoint solutions with such firms as iDevFactory and Booz Allen Hamilton. Her applicable knowledge and understanding of the underlying SharePoint security has allowed her to provide many organizations with meaningful and enforceable policies for their SharePoint environments. She offers a realistic business look into management of SharePoint security today.

For additional information or to download a 14-day evaluation of any Idera product, please visit: www.idera.com.

ABOUT IDERA

Idera provides tools for Microsoft SQL Server, SharePoint and PowerShell management and administration. Our products provide solutions for performance monitoring, backup and recovery, security and auditing and PowerShell scripting. Headquartered in Houston, Texas, Idera is a Microsoft Gold Partner and has over 5,000 customers worldwide. For more information, or to download a free 14-day full-functional evaluation copy of any of Idera's tools for SQL Server, SharePoint or PowerShell, please visit www.idera.com.

Idera | BBS Technologies | 802 Lovett Blvd Houston, Texas 77006
PHONE 713.523.4433 | TOLL FREE 877.GO.IDERA (464.3372)
FAX 713.862.5210 | WEB www.idera.com

