


A background image showing a laptop on a desk with a circular gauge overlay. The gauge has numbers from 0 to 60 and a needle pointing towards 40. The scene is dimly lit, suggesting an office environment.

Microsoft® SharePoint® Use Models and Security Risks

Trend Micro, Incorporated 

 This white paper examines the increasing risks to SharePoint and offers best practices to ensure optimal security.

A Trend Micro White Paper | April 2010

➔ TABLE OF CONTENTS

I. A BRIEF INTRODUCTION TO MICROSOFT® SHAREPOINT®	3
II. SHAREPOINT USE AND RISKS.....	3
THREATS ARE MORE MALICIOUS	4
EMPLOYEES ARE MORE MOBILE.....	5
SHAREPOINT IS NOT JUST USED BY EMPLOYEES.....	5
SHAREPOINT IS NO LONGER JUST A REPOSITORY.....	5
EASE OF WEB 2.0 USE CAN INVITE UNWANTED CONTENT.....	6
III. ASSESSING YOUR RISK	7
IV. COMMON USE MODELS AND RELATED RISK.....	8
EMPLOYEE CONTENT MANAGEMENT AND COLLABORATION.....	8
EXTENDED CONTENT MANAGEMENT AND COLLABORATION.....	9
OPEN COLLABORATION	9
V. CONCLUSION	9
FIVE KEY QUESTIONS TO ASK.....	10
BEST PRACTICE SECURITY RECOMMENDATIONS.....	10

I. A BRIEF INTRODUCTION TO MICROSOFT® SHAREPOINT®

Microsoft® SharePoint® 2010 is the latest version of server-based collaboration software from Microsoft, promising to connect people, processes, and information. It comprises two main components: 1) the core Microsoft Windows® SharePoint Services (WSS 4.0), which include the content repository, libraries, and services, making it accessible to a distributed user population and applications; and 2) the Microsoft SharePoint Server (formerly called MOSS), which encompasses a number of applications and interfaces on top of the repository.



With 2010 version, organizations are provided with more and more capabilities above and beyond the basic content repository for which it was first used.

II. SHAREPOINT USE AND RISKS

Without question, these new collaboration capabilities are valuable to business. Improved remote or regional communication, increased speed of decision making, and reduced in-person meetings and travel expenses are all cited as important business benefits of SharePoint deployments in the U.S. and Europe.¹ However, it is important to recognize that new capabilities also give rise to new security risks.

Traditionally, SharePoint was primarily a central repository for employees to share files within the corporate network, and the security risks stemmed from viruses and worms self-propagating across and within networks. Such attacks tied up network bandwidth, slowed access to systems, and impaired employee productivity. And unlike today, these attacks were highly visible, and their impact was limited to a defined period.

¹ Osterman Research. "SharePoint Use Survey." December 2008.

Threats Are More Malicious

Today, profit-driven threats are hidden, operating in stealth mode in order to steal your data. The attacks are significantly more harmful, sophisticated, and insidious. For example, recent exploits of vulnerabilities in the Microsoft operating system have allowed worms such as Downad.A to propagate among PCs and servers, including those running SharePoint. These threats are designed to steal user names and passwords, and often install additional web-based malware components that steal other sensitive data.²

At the same time, file-based malware with a high degree of social engineering has become commonplace. We routinely see emails claiming to include business-oriented attachments—such as package delivery notices,³ contracts,⁴ and software updates from IT support⁵—which are, in reality, malicious files. At the same time, we also see emails offering innocuous attachments—like an Olympics schedule—but these files also contain embedded malware hidden within them.⁶ This hidden malware then exploits vulnerabilities in applications to automatically execute without user action or knowledge.⁷ This trend is particularly worrisome since, according to the SANS Institute, a leading provider of security training courses, file vulnerabilities like those in Microsoft Office or Adobe® PDF files, are the first choice of attackers for zero-day attacks.⁸ No matter how the malware is disguised, it only requires one user to take the bait and allow malware to enter your SharePoint environment.

But that's not all. When organizations choose to utilize SharePoint's web-based capabilities—portals, team sites, wikis, and blogs—especially those that are external-facing, they must be concerned about a whole new class of threats: web threats. Many of these threats take advantage of SQL injection, Cross-site Scripting, and other techniques to embed malicious code in legitimate web pages and redirect users to malicious sites. From there, malware often automatically downloads to the victim's PC and/or steals data.⁹ This is the fastest-growing class of threats and one that is increasingly programmatic rather than targeted.

In addition to the risk of a SharePoint web page compromise, organizations need to be wary of users unknowingly posting links to compromised sites. Popular news sites are frequently targeted for their high volume of organic traffic. According to SANS, "Attacks against web applications constitute more than 60% of the total attack attempts observed on the Internet. These vulnerabilities are being exploited widely to convert trusted web sites into malicious websites serving content that contains client-side exploits."¹⁰

According to the Computer Security Institute, the average cost of security incidents in 2009 was \$234,244¹¹, and in many cases even a single compromise can have a far-reaching impact.

² Trend Micro, "DOWNAD/Conficker Turns 1yr." February 2010.

³ Trend Micro, "Laptop Delivery Note Contains Malware," August 2009.

⁴ Trend Micro, "Zbot Spam Campaign Continues," October 2009.

⁵ Trend Micro, "Trojanized Doc Files in Targeted Attack," January 2008.

⁶ Trend Micro, "Let the Games Begin," July 2008.

⁷ SANS Institute, "Top Security Risks," September 2009.

⁸ Trend Micro, "Total Recall: The Month of Mass Compromises," May 2008.

⁹ SANS Institute, "Top Security Risks," September 2009.

¹⁰ Computer Security Institute, "Computer Crime and Security Survey," December 2009.

¹¹ Osterman Research, "The Need for SharePoint Security," April 2010.

Employees Are More Mobile

In the past, SharePoint users were often perceived to be safe within a secure perimeter—working inside a corporate network, protected by layers of security such as email and endpoint security. As most of us know, this is no longer the case. Employees are increasingly mobile or remote. They often use PCs at home for business and personal use. Organizations understand that there is no such thing as a “secure perimeter” and that employees are often outside the corporate network, protected by only one layer of protection—their endpoint security. Unfortunately, this is unreliable since endpoint security may become outdated or circumvented when the mobile user is outside of the network.

SharePoint Is Not Just Used By Employees

A wide range of external parties is increasingly a part of SharePoint communities. Independent contractors or consultants are often hired on a one-time or recurring basis. Affiliates and franchisees may play an important role in an organization’s daily business operations. Business partners, suppliers, and other vendors are often key collaborators granted access to a SharePoint community. And of course, customers often have access to extranet sites that are part of an organization’s SharePoint environment. An Osterman Research survey of enterprises in North America and Europe found that 48% of organizations provide SharePoint access to contractors/consultants, 38% collaborate with business partners, 31% include affiliates, and 19% welcome customers into their SharePoint community.¹²

In all such cases, endpoint security is generally outside of the organization’s control, giving rise to two separate concerns. 1) Have all SharePoint users taken appropriate measures to ensure that their PCs are free of malware, which could otherwise be introduced to the SharePoint community? 2) If malware enters the SharePoint community, can their security be relied upon to stop it, and if it does, what would be the impact when users (especially affiliates, partners, and customers) see malware circulating within the organization’s SharePoint community?

SharePoint Is No Longer Just a Repository

According to Gartner, Web 2.0 technologies are expected to have a “transformational impact” on organizations in the next two years.¹³ This can be seen in the growing use of SharePoint capabilities beyond content management. While 71% of organizations participating in a recent market survey reported that they do use SharePoint for content management, 65% indicated that they use team sites, 41% will use wikis and blogs, and 35% will use external portals.¹⁴ While these rich capabilities increase collaboration, they do give rise to additional risks given the exponential increase in web threats, including the growth in compromised sites as a result of programmatic cybercriminal activity.

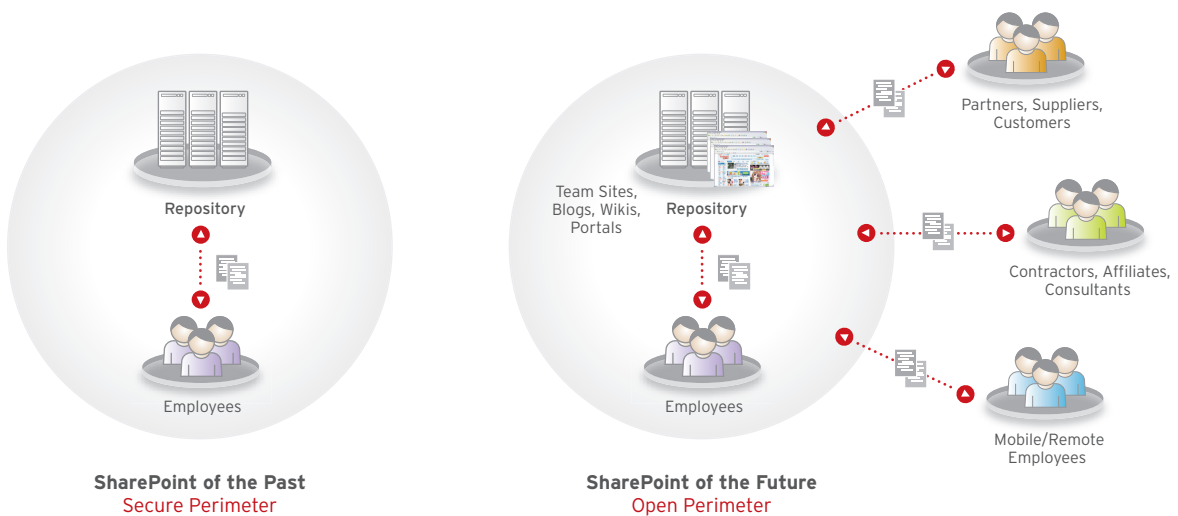
¹² IT News, “Gartner Throws Weight Behind Web 2.0,” August 2008.

¹³ Osterman Research, “The Need for SharePoint Security,” April 2010.

¹⁴ Dallas Morning News, “American Pilots Protest Security Breach On Company Web Site,” June 2007.

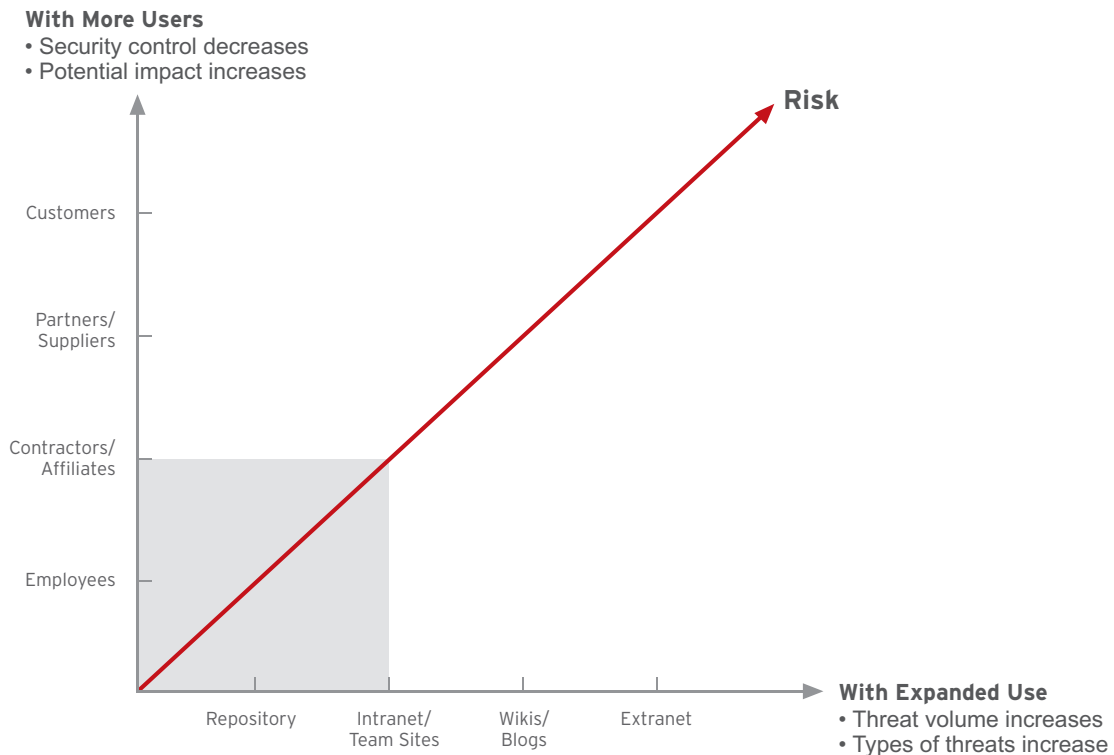
Ease of Web 2.0 Use Can Invite Unwanted Content

The familiarity of blogs, wikis, and discussion forums make it easy for users to communicate more effectively but also may tempt to users to forget where they are posting. Profanity or racist language could enter into a discussion which can not only destroy the trust you are trying to build but also result in a lawsuit if the organization does not take steps to prevent this type of abuse. Further, files containing personal information such as credit card numbers or social security numbers could be accidentally posted to a SharePoint site exposing this information. In 2007, an American Airlines employee inadvertently posted a file containing the names and social security numbers of over 300 employees to the company's intranet¹⁴. The risk of an accidental posting such as this one is a costly data breach which can result in fines and loss of goodwill.



III. ASSESSING YOUR RISK

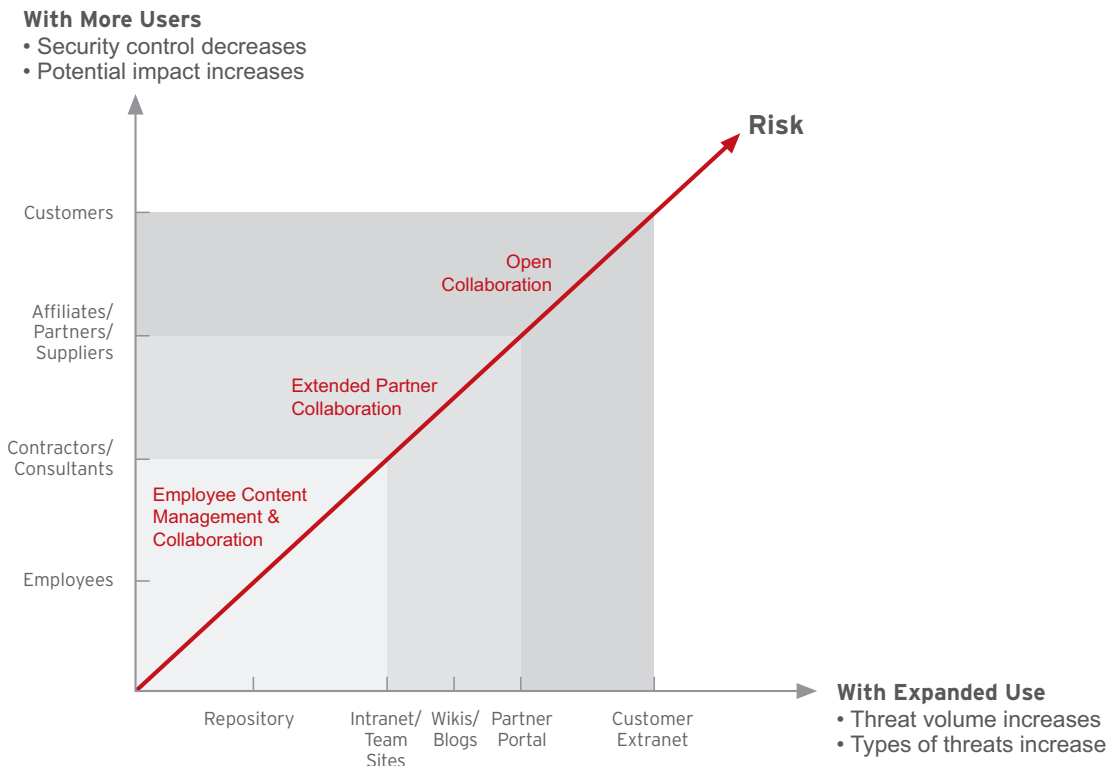
The bottom is that there are a variety of challenging factors beyond IT control, including: 1) the continually evolving threat landscape, 2) the sophistication of cybercrime, 3) increased employee mobility, and 4) the inclusion of non-employees that are outside of IT control. With these factors in mind, it is best to focus on areas that can be controlled, like the type of users that are allowed in your SharePoint environment and the SharePoint capabilities being used. Once the level of risk and risk sources are understood, organizations can weigh the risks vs. benefits and take action to mitigate certain risks as appropriate.



IV. COMMON USE MODELS AND RELATED RISK

Customers are generally using one of three common mixes of SharePoint capabilities, or use models. For the purpose of this paper, these use models fall into one of three areas on the risk chart:

- **Moderate risk:** employee content management and collaboration
- **Heightened risk:** extended partner collaboration
- **Highest risk:** open/external collaboration



Employee Content Management and Collaboration

SharePoint adoption has grown out of the need to replace traditional file sharing servers. The business limitations of file sharing include a lack of document management, version control, and ability to lock a document while one person is editing. Windows SharePoint Services (WSS) overcomes these and other limitations to help employees collaborate. It is common for pseudo-employees, such as independent contractors and consultants, to be granted access to the SharePoint repository, or at least segments of the repository.

There comes a time when the basic content repository is no longer sufficient, especially as teams become geographically dispersed and/or virtual. In such cases, the need to collaborate in one central location is paramount for optimal efficiency. Enter team sites, which allow separate groups to have their own space to collaborate in one central location with tasks, document sharing, contacts, events, and other information.

Once teams start using SharePoint Server to collaborate, organizations tend to recognize a heightened sense of possibility. Capabilities like full site search and basic project management further raise team efficiency. At the same time, the portal provides the ability to control the look and feel of your personal, divisional, and organization-wide intranet sites. Functions like “My Personal Site” allow end users to post information about themselves for business or personal community building.

Now that your employees have rich, web-based front ends for the repository—as well as a plethora of web-based collaborative tools, what is the next step? Online business process, intelligence, and forms are tools that allow you to structure employee content creation, guide workflow, and generate reports.

Extended Content Management and Collaboration

It's clear that employee collaboration has improved productivity and innovation, but other parties have important roles to play in your business. What do you do to accommodate them? Many organizations expand their SharePoint community to include affiliates and partners who directly contribute to business success—either as full users (albeit access-controlled) or limited users with access to specific resources through a partner extranet.

Partners' roles determine their level of access. In some cases, they are tightly woven into strategic activities (such as design or development partners in the manufacturing sector) and need full access to collaborative systems and resources. In other cases, partners may be a key route to market, but operate as more of a resource consumer enabled by an externally-facing portal rather than a contributor collaborating through a dedicated segment of SharePoint. In many cases, wikis and blogs are excellent ways to share information and introduce a degree of partner interactivity without granting them full access to SharePoint.

Open Collaboration

External portals are increasingly used to communicate with customers, especially among business-to-business service providers (like those offering payroll or human resource services). These portals provide controlled access to a subset of SharePoint resources and capabilities. Some organizations even utilize extranets, not to mention wikis and blogs, to welcome customers into areas of their SharePoint community. According to recent market research, roughly one in five organizations in North America and Europe include customers in their SharePoint community.¹⁵

V. CONCLUSION

With more interactive SharePoint capabilities, expanded use beyond employees, and the growing sophistication of threats, the risks have escalated exponentially. The potential costs of a security incident include data theft, data loss, reputation damage, downtime, and lost business. With these high stakes, SharePoint security is critical. So what can you do about it?

¹⁵ Osterman Research, “The Need for SharePoint Security,” April 2010.

Five Key Questions to Ask

Start by answering five key questions that identify your risk, determine your willingness and ability to handle that risk, and consider the measures required to reduce your risk to a level you find acceptable.

- 1) What SharePoint capabilities (repository, intranet portal, team sites, wikis and blogs, extranet portals, etc.) are being used?
- 2) Who (employees, contractors, affiliates, business partners, customers, etc.) is using them?
- 3) What security risks and potential impacts/costs accompany these capabilities and users?
- 4) What is an acceptable security risk, given the potential costs of security measures to manage them?
- 5) For those risks I want to address, what is the best way to reduce them with minimal cost and complexity?

Best Practice Security Recommendations

Unfortunately, there is no “one-size-fits-all” solution to SharePoint security, nor any 100% guarantee behind it. However, there are a number of effective, easy-to-manage ways to minimize risk without impeding essential business collaboration.

- 1) For those seeking the most basic security, start by protecting the underlying OS of your SharePoint servers against worms and other attacks by deploying server antivirus—such as Trend Micro™ OfficeScan™ Server Edition, or Trend Micro™ ServerProtect™—and keeping them up to date with the latest patches. Also consider implementing an Intrusion Prevention System (IPS) to protect the OS before patches are available.
- 2) For those concerned about SharePoint users and data, it is important to protect the repository, portals, and other components of SharePoint by blocking file-based malware, web threats, and filtering content with SharePoint-specific security—above and beyond basic file server antivirus. This is where Trend Micro™ PortalProtect™ can help customers today.
- 3) Define your most sensitive data and control access to it based on SharePoint permission. You can also control how SharePoint is used by instituting content filtering or data leak prevention technology. (Remember that no administrator or user should have full permissions over all content.)
- 4) Keep your SharePoint infrastructure—backend SQL database and front end web sites—patched and properly configured to check application and user access permissions. You should also consider an extra level of web threat protection. Trend Micro PortalProtect checks links in real-time and blocks URL's before they are posted.
- 5) While back-up solutions are common for SharePoint systems, they are rarely used. They should therefore be routinely tested to ensure that they continue to work properly.

TREND MICRO™

Trend Micro Incorporated is a pioneer in secure content and threat management. Founded in 1988, Trend Micro provides individuals and organizations of all sizes with award-winning security software, hardware and services. With headquarters in Tokyo and operations in more than 30 countries, Trend Micro solutions are sold through corporate and value-added resellers and service providers worldwide. For additional information and evaluation copies of Trend Micro products and services, visit our Web site at www.trendmicro.com.

TREND MICRO INC.

10101 N. De Anza Blvd.
Cupertino, CA 95014

U.S. toll free: +1 800.228.5651

phone: +1 408.257.1500

fax: +1 408.257.2003

www.trendmicro.com

