The Need for SharePoint Security

An Osterman Research White Paper

Published April 2010

SPONSORED BY

Osterman Research, Inc. • P.O. Box 1058 • Black Diamond, Washington 98010-1058
Tel: +1 253 630 5839 • Fax: +1 253 458 0934 • info@ostermanresearch.com • www.ostermanresearch.com

Summary

METHODOLOGY

Osterman Research conducted a survey with 235 individuals in March 2010, most of whom are located in North America. The goal of this research was to determine, among other things, the penetration of Microsoft SharePoint in organizations of all sizes. The mean number of employees and email users at the organizations surveyed was 11,179 and 10,216, respectively; medians were 300 and 308, respectively.

Earlier, Trend Micro commissioned Osterman Research to undertake a survey of North American and European organizations to determine how and why they are using Microsoft SharePoint and to determine their requirements for security specifically focused on SharePoint. A total of 269 surveys were completed with individuals who are involved in managing the messaging and collaboration infrastructure for their organizations. The countries surveyed included respondents in North America (104 completed surveys), France (44), Germany (45), Sweden (45) and the United Kingdom (31). The mean number of employees and email users at the organizations surveyed was 11,228 and 9,632, respectively; medians were 2,500 and 1,500, respectively.

To qualify for the second survey, respondents' organizations had to be a) using SharePoint 2007 or Windows SharePoint Services 3.0, b) they plan to use SharePoint 2007 during the next 12 months or c) they use SharePoint 2003 or Windows SharePoint Services 2.0 and have no plans to upgrade to SharePoint 2007 or Windows SharePoint Services 3.0. Organizations that do not use or plan to use SharePoint were disqualified from completing the survey.

IMPORTANT TAKEAWAYS AND OBSERVATIONS

There are a few important takeaways from the research findings:

- For many organizations, Osterman Research found that SharePoint security is considered a "nice to have", but that security capabilities deployed at the gateway, server and endpoint level are perceived to be sufficient to protect SharePoint servers from malware and related threats. However, deploying anti-malware software at the endpoint or on a server does not actually secure the SharePoint environment (the underlying database, Web pages, etc.) Organizations should understand that deploying SharePoint security at all layers of the network and on all systems is key to protecting a network from all threats.

- Where they do exist, the focus of SharePoint security concerns appears to be much more focused on protecting sensitive information than on traditional malware and similar threats. There was somewhat more concern about security for SharePoint from an information-protection perspective in Europe which, we believe, is related to the much greater emphasis on information privacy in Europe than in North America.

- However, stopping malware and managing data leaks are related problems. Because many data leaks are caused by malware, such as keystroke loggers, stopping malware within the SharePoint environment is an important component in addressing issues surrounding information protection, a fact that many decision

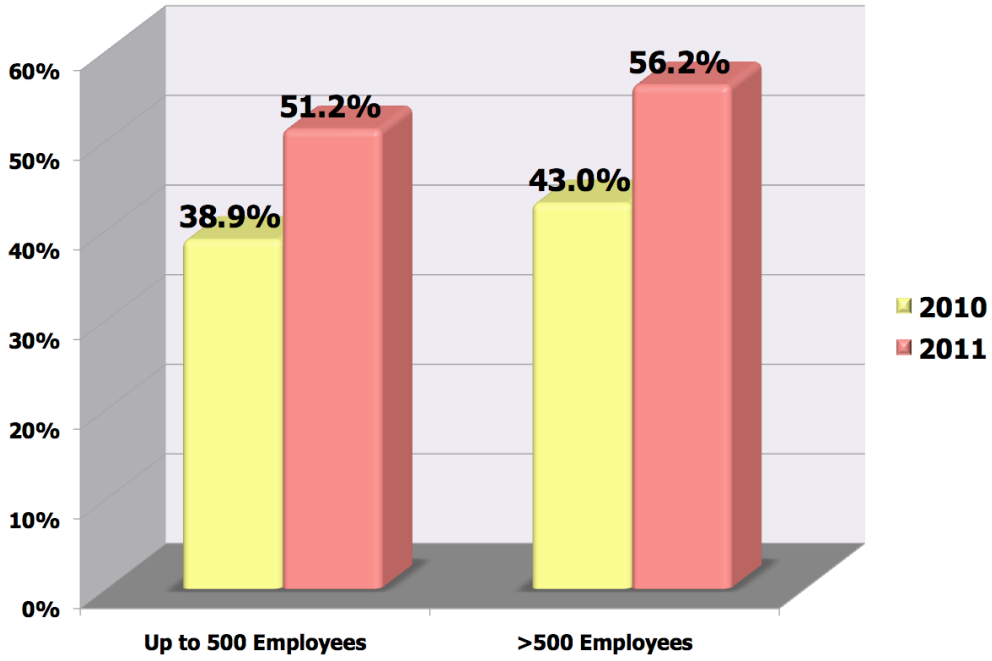
makers in our survey may not yet fully appreciate.

- Employees are the most common SharePoint users with a mean of 95% of organizations reporting that this group uses or would use SharePoint. Contractors and consultants are more likely to use SharePoint in North America compared to Europe, while affiliates are generally more likely to use it in Europe. This, too, underscores the need to protect SharePoint from a variety of threats, since use of SharePoint by those beyond the firewall can introduce a variety of threats completely outside the control of in-house IT staff.

- Regulatory issues, including increased corporate oversight will be a key issue that may drive some organizations to deploy SharePoint security, particularly for content protection-related issues. This will be particularly important over the next 24 months, as organizations in the financial services industry, among others, become the targets of increased regulatory oversight.

SharePoint is Becoming a De Facto Standard in Exchange-Enabled Organizations

In the March 2010 survey conducted by Osterman Research, we found current penetration of SharePoint at 39% of email users in Exchange-enabled organizations of up to 500 users – in larger Exchange-enabled organizations, 43% of email users employ SharePoint. The survey also found that SharePoint use will grow significantly – to 51% of users in smaller organizations and 56% in larger ones, representing growth of more than 30% in just 12 months, as shown in the next figure, despite a continuing soft economy.



The research conducted for the earlier survey found that only 60% of organizations that use or plan to use SharePoint currently have security on their SharePoint servers. Another 25% plan to do so during 2009.

SHAREPOINT USE VARIES WIDELY

The research found that 37% of organizations report that SharePoint is used, or will be used, by all users who have email – the figure in German companies was a high of 47% and in Sweden it was a low of 29%. Another 18% of organizations report that SharePoint is or will be used by most email users, while another 24% report that SharePoint is or will be used by certain groups or departments that are enterprise-wide. Only 8% of organizations report that they are just testing or piloting SharePoint, indicating that SharePoint has become a key part of the infrastructure at the organizations surveyed.

REASONS FOR USING SHAREPOINT ARE VARIED

There are a variety of reasons cited by organizations for using SharePoint, including improvement of remote or regional communication (74%), improvement in the speed of decision making (56%), reducing in-person meetings and travel expenses (55%) and improving communication with external partners or vendors (34%).

We found some interesting differences between the North American and European audiences we surveyed:

- Improving remote or regional communication was a slightly more important reason for using SharePoint for European respondents (77%) versus North American ones (71%).

- Reducing in-person meetings and travel expenses was also more important for Europeans (59%) versus North American respondents (50%).

These findings are not surprising given the higher costs for travel within Europe and the language differences that continue to vex European business decision makers.

It is important to note that reasons for SharePoint vary widely, including portal development, search capabilities, content and document management control, the development of business forms, business intelligence applications and other uses.

WEB COLLABORATION IS BECOMING MORE COMMON

Web-based collaboration tools focused on document sharing, wikis, blogs, project management and other collaborative capabilities are increasingly used in organizations of all sizes.

Among organizations that use or plan to use SharePoint 2007 or Windows SharePoint Services 3.0:

- North American organizations are much more likely to use team sites (80%) versus European organizations (58%).

- North American organizations are also more likely to use wikis, blogs and other collaboration features (52%) than Europeans (34%).

- North American organizations are also more likely to use the content management features of SharePoint (76%) versus Europeans (68%).

We're not completely sure why these differences exist, but the reasons for them are not likely because of any significant differences in penetration between in SharePoint use among North American and European organizations – we found current and planned penetration of SharePoint to be roughly similar across both groups. Instead, we believe that corporate culture may be the primary reason for these somewhat significant differences.

DOES SHAREPOINT REPLACE EMAIL?

One of the primary applications for SharePoint is as a document repository. As such, we would expect that the use of email in SharePoint-enabled applications would go down as more documents were being distributed in and managed with SharePoint. However, the March 2010 survey found just the opposite: organizations that have deployed SharePoint send and receive substantially more emails than their counterparts that do not use SharePoint. We believe that the primary reason for this somewhat counterintuitive finding is that organizations that have been the earlier adopters of SharePoint are more focused on information management, and so continue to use SharePoint alongside email, not as a replacement for it. In other words, information-intensive corporate cultures are more likely to deploy SharePoint as exemplified by their heavier use of email.

SharePoint Security is a Must-Have

SHAREPOINT SECURITY IS HIGHER IN EUROPE

Among North American respondents, 58% of respondent organizations have deployed security on their SharePoint servers and another 27% plan to do so during the next 12 months. Among European respondents, 62% have done so and 24% plan to deploy security during the next 12 months. Interestingly, while 11% of North American respondents indicated that they have not deployed SharePoint security and have no plans to do so, this figure is only 2% in Europe.

North American respondents cited protection of sensitive information (69%) as the primary reason for deploying SharePoint security, while 74% of European respondents indicated this was the primary reason. Malware is less of a driver for deploying SharePoint security among North American organizations (37%), but was more important in Europe with a mean of 48% of organizations citing malware as the reason for SharePoint security.

Underscoring the critical need for security in corporate SharePoint environments is the fact that many SharePoint users are outside of corporate IT's control. For example, 31% of organizations allow affiliates to use SharePoint, 38% allow business partners, 48% allow contractors or consultants and 19% allow customers to use SharePoint. The

security for each of these groups is clearly outside the control of IT in most cases, leaving organizations that have not deployed SharePoint-specific security vulnerable to whatever security (or lack of security) that might exist in each of the environments that has access to their SharePoint infrastructure.

OUTSIDE USERS NECESSITATE MORE EMPHASIS ON SECURITY

Interestingly, the higher proportion of European organizations that have deployed SharePoint security coincides with the generally greater European use of SharePoint by affiliates, business partners and customers. The use of SharePoint by contractors and consultants is slightly higher in North America than in Europe. Because many of these individuals work behind the corporate firewall of the organizations that engage them, this may leave corporate decision makers with the notion that SharePoint security is less critical than if external parties are using SharePoint.

Corroborating this theory is the fact that among North American organizations in which only employees use SharePoint, 55% have enabled SharePoint security; among North American organizations in which affiliates, business partners and customers use SharePoint, 61% have deployed security. We found little difference in the two populations among European organizations overall.

Summary

SharePoint use is on the increase, due in part to its efficacy for team sharing, document management, portal development and other uses; and also due to Microsoft's aggressive licensing policies for SharePoint. However, many organizations have not deployed SharePoint-specific security, instead relying on security deployed at the endpoints of the network, on servers or on gateways. Given that a large proportion of organizations allow external users to access their SharePoint infrastructure, this leaves them vulnerable to a variety of threats, including malware infections and loss of data. As a result, organizations that have deployed SharePoint should also deploy SharePoint-specific security capabilities.