

# Results of an Osterman Research Survey on Web Security

**An Osterman Research Survey Report**

*Published January 2009*

**SPONSORED BY**



## Survey Findings

---

### BACKGROUND AND METHODOLOGY

Osterman Research conducted a survey, commissioned by Purewire, to understand the problems and issues that organizations are having with employee use of the Web and Web applications. The online survey was conducted with 139 respondents who are knowledgeable about their organization's use of Web tools and applications.

The median number of employees at the organizations surveyed was 1,000 and the median number of Web/Internet users was 852. The survey was conducted during November 2008. A median of 20% of users at the organizations surveyed works remotely at least part of the time and 15% regularly access the Web from a mobile phone or PDA.

### THE WEB IS FRAUGHT WITH RISKS

The survey discovered that use of the Web carries with it a number of quite serious risks and potential risks and organizations are very concerned about these risks. Among the findings were the following:

- A plurality of organizations (46%) estimates that these infections came from users visiting infected Web sites, 25% felt they came from email, while 16% said they came from another source. A mean of 9% of organizations – one out of every 11 – had remote workers' computers infected with malware, spyware or related problems during the previous 12 months.
- Seventy-six percent (76%) of organizations are concerned or very concerned that the Web is an entry point for malware.
- Fifty-five percent (55%) are concerned or very concerned about the impact that the Web and Web security have on network bandwidth.
- Forty-nine percent (49%) are concerned or very concerned about enforcing Web usage and Web security policies for employees that work remotely, such as ensuring that they do not visit undesirable URLs or that they are not exposed to malware via the Web.
- Forty-eight percent (48%) are concerned or very concerned about supporting remote workers with various Web applications.
- Forty-four percent (44%) are concerned or very concerned about employee productivity losses from Web surfing.

Of all organizations that had remote workers' computers infected with malware, spyware or related problems during the previous 12 months, 46 percent estimates that these infections came from users visiting infected Web sites.

The bottom line is that the Web and Web applications pose a serious conundrum: the productivity gains and cost savings from use of these tools can be significant and will become more important given the pressures resulting from the current economic crisis, but these tools create enormous risk for organizations of any size.

## WHAT ORGANIZATIONS ARE DOING IN RESPONSE

The vast majority of organizations surveyed (79%) have established corporate policies against downloading certain types of files, while nearly as many (76%) have deployed systems that will actively block downloads of certain file types. Others have implemented a variety of tools, policies and systems to protect against Web-borne threats. Ironically, and despite the significant growth and dynamic changes happening on the Web and the longevity of traditional URL filtering technology, nearly 40 percent of those surveyed do not have these simple URL filtering solutions in place, though many are using a policy enforcement/reporting solution for Web use at the global, group or individual user level.

Sixteen percent attempt to lock down employee desktops, but admit they have less than complete success in doing so; 12% admit to not being completely successful in their attempts to lock down laptops against Web threats.

Many organizations have implemented tools to control the use of Web applications, including blocking and/or monitoring the use of Web applications at the firewall (69% of organizations), use of a security Web gateway to monitor the use of Web applications without blocking their use (31%) and use of a secure Web gateway to prevent users from installing Web applications. However, URL filters alone or policies to restrict use of Web applications cannot block applications that are streaming, leaving the network vulnerable to attacks from Web 2.0 objects.

## THE WEB IS A POTENTIAL SOURCE OF DATA LOSS

Malware and even user of legitimate Web applications can allow confidential or otherwise sensitive information to be leaked in ways that could potential be damaging to an organization. Seventy-one percent of organizations have established policies that are designed to prevent data loss, while 25% monitor outgoing content without blocking it, and only 18% are using some sort of data loss prevention (DLP) solution. One in 10 organizations are not using any sort of solution to protect against data loss.

## MANY SOLUTIONS AND PRACTICES ARE FALLING SHORT

The survey found that 46% of organizations lock down employee desktops so that users cannot install certain Web applications, while 39% do so for employee laptops. Interestingly, another 16% attempt to lock down employee desktops, but admit they have less than complete success in doing so; 12% admit to not being completely successful in their attempts to lock down laptops against Web threats.

## WHAT ABOUT USING SaaS SOLUTIONS?

Many organizations are using software-as-a-service (SaaS) solutions to protect their infrastructure. For example, 71% of organizations are using SaaS-based anti-virus/anti-spam capabilities (although not for all users), 26% are using SaaS-based archiving solutions, and 26% are using SaaS-based Web security solutions.

The majority of organizations (58%) do not have an organization-wide mandate or strategy to move in the direction of SaaS-based solutions for various parts of their infrastructure, but 19% of organizations do have some sort of mandate to migrate to SaaS-based solutions. Other Osterman Research surveys have confirmed the growth of the SaaS-based paradigm, particularly given challenging economic times in which decision makers will be evaluating less costly and more efficient methods managing key parts of their infrastructure.

## ORGANIZATIONS ARE LOOKING FOR THE BENEFITS THAT SaaS-BASED SOLUTIONS CAN PROVIDE

We also asked decision makers about the characteristics of Web security solutions that they felt would offer a benefit or significant benefit. Among the more important characteristics were keeping threats out of the network (cited by 87% of respondents as a benefit or great benefit), instant access to security updates (77%), low maintenance requirements (75%), predictable pricing (71%) and not having hardware and software to purchase or deploy (59%).

These are among the most important benefits that SaaS-based solutions can provide, whether for Web security systems, email-oriented security systems, customer relationship management systems and the like. These benefits will assume even greater importance during 2009 given that the economy will allow only 9% of the organizations surveyed to increase their security technology purchases, while another 22% will be decreasing security-related purchases.

While IT security budgets are likely to remain consistent or even decrease during 2009, SaaS-based Web security solutions offer the double benefits of being highly effective against the latest generation of Web threats, while offering low up-front costs and predictable pricing.

Further, the survey found that given the balance between security and performance, decision makers tend to lean toward security. For example, when asked to rate their desired balance between security and performance on a scale of 1 (total focus on security) to 7 (total focus on performance), 51% chose a more security-oriented option, while 21% chose a more performance-oriented solution; 28% were evenly split between security and performance.

## KEY TAKEAWAYS

There are several important takeaways from the survey findings:

- The Web and Web-based applications are incredibly useful tools that carry with them enormous risk of infection from a growing variety of threats. Even legitimate, business-oriented sites can become infected with malware and create significant risks for any organization.
- The risks posed by Web-related threats are not theoretical – they are impacting organizations and users today.
- Organizations have generally been fairly responsive in terms of establishing policies that are designed to protect their organizations from Web-related threats, but have generally not been as quick to implement effective tools to protect their infrastructure.
- Many of the solutions that have been implemented are simply not adequate to meet the growing number or dynamic nature of current threats.
- SaaS-based Web security solutions offer the double benefits of being highly effective against the latest generation of Web threats, while offering low up-front costs and predictable pricing.

© 2008 Osterman Research, Inc. All rights reserved.

No part of this document may be reproduced in any form by any means, nor may it be distributed without the permission of Osterman Research, Inc., nor may it be resold or distributed by any entity other than Osterman Research, Inc., without prior written authorization of Osterman Research, Inc.

Osterman Research, Inc. does not provide legal advice. Nothing in this document constitutes legal advice, nor shall this document or any software product or other offering referenced herein serve as a substitute for the reader's compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, administrative order, executive order, etc. (collectively, "Laws")) referenced in this document. If necessary, the reader should consult with competent legal counsel regarding any Laws referenced herein. Osterman Research, Inc. makes no representation or warranty regarding the completeness or accuracy of the information contained in this document.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.