Microsoft GOLD CERTIFIED Partner

GFI

Survey: Web filtering in Small and Medium-sized Enterprises (SMEs)

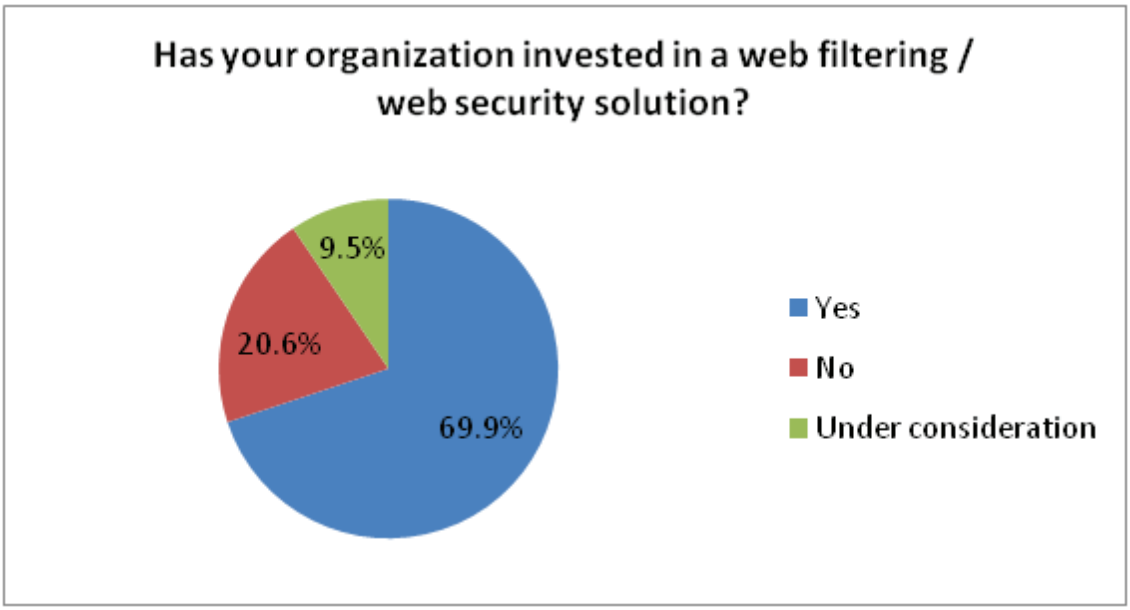
September 2010

More and more organizations are seeing value in web filtering and web security solutions, a survey conducted by GFI Software shows, with seven in 10 stating they use technology to monitor and control Internet access by employees.

The growing threat from web-based malware and phishing attacks is pushing businesses to adopt technology that can help them to control not only what sites their employees are visiting during office hours but also what files they are downloading.

A survey by GFI last year found that only 47% of US SMEs had the means to monitor and / or filter HTTP traffic, even though 61% had security policies regarding Internet use in place.

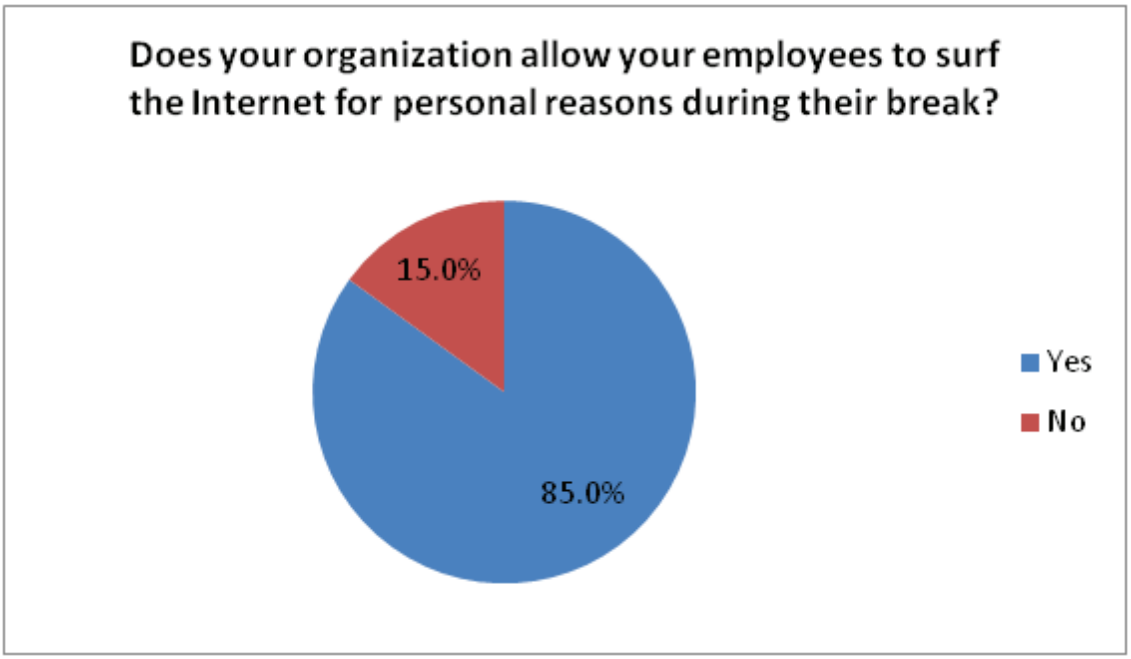
GFI's latest survey, however, shows a positive increase in the number of SMEs that are monitoring and/or filtering HTTP traffic (69.9%). Factoring in those who are currently considering the investment, the percentage goes up by another 9.5%.



N=631

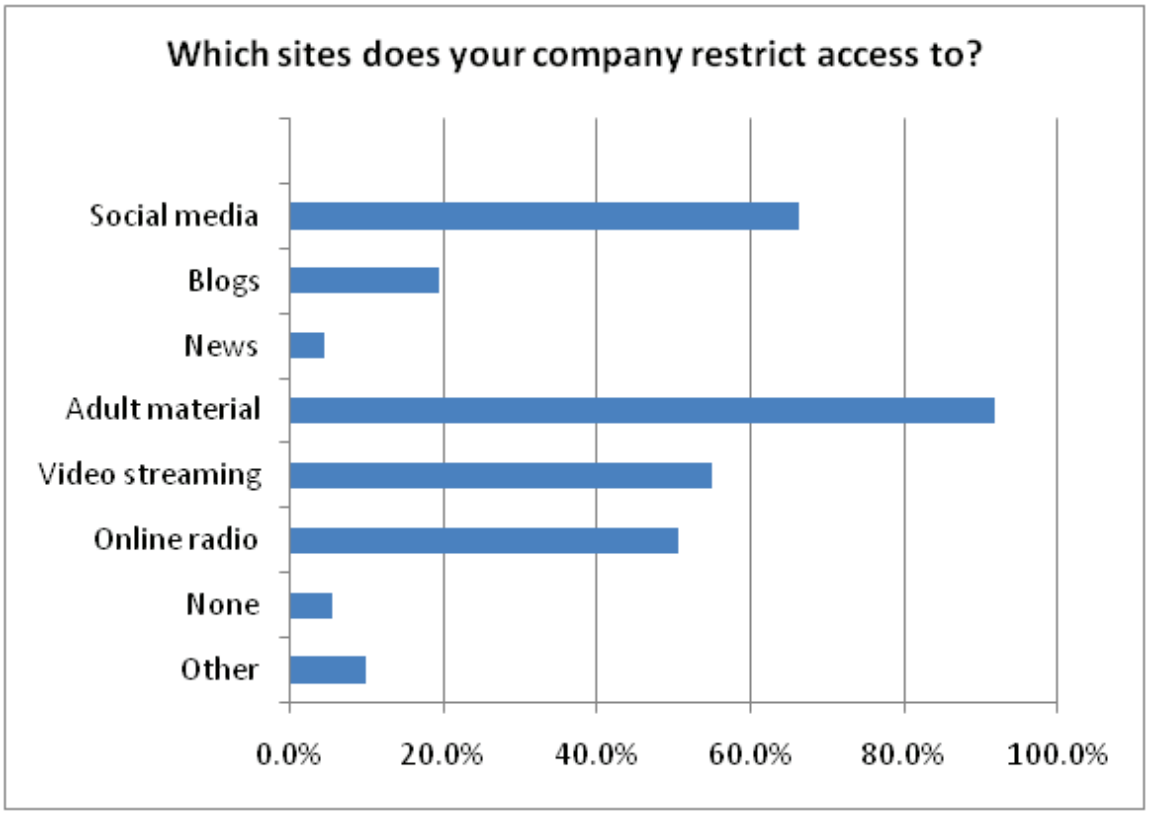
There are two possible reasons for this positive change. First, the growing incidence of malware infections and successful phishing attacks are a concern for many organizations, hence their need to monitor and control Internet use, especially downloads. Second, most employees have a social media account that they invariably update or read during office hours, thus impacting on productivity and bandwidth resources. Time is money and organizations do not want their employees wasting time at the company's expense.

When asked why they had invested in a web filtering and web security solution, 9 in 10 SMEs said they did so to block inappropriate content, to prevent malware infections from downloaded files and to prevent malware attacks via drive-by downloads. More than half said they wanted to reduce cyberslacking, to control what sites employees can or cannot visit and to reduce bandwidth costs associated with unnecessary browsing/streaming.



N=427

The GFI survey also shows that although companies have not banned Internet access and 85% of those using web filtering / web security solutions allow their employees to surf the Internet for personal reasons during their break, there are restrictions on what can be viewed and what sites can be accessed. Adult material tops the list followed by social media sites. Next in line are video streaming websites and online radio.



N=427

While organizations are happy to allow employees to access the Internet for personal reasons, they are not giving them access to sites that are known to contribute most to loss in productivity / cyberslacking and those sites that are bandwidth-hungry. It also may be the case that organizations are only allowing access at certain times of the day, for example, during employees' lunch break or after hours. Blogs and news sites are the categories of websites blocked the least by respondents to the survey.

It is also encouraging that nearly 80% of respondents said their company had a written and clearly defined 'Web Acceptable Use Policy' and over 92% said their employees are aware that their online activity is being monitored.

Although three in 10 do not have the means to monitor and control Internet use in the organization, the reasons given for not doing so indicate that these organizations do understand the need to address web-based threats. Of those organizations that have not made the investment, only 24% said they do not see the need for such a product. However, 22% said the purchase had not been approved by management or they did not have the budget while just over 38% said they had considered the investment but have higher priorities.

Nearly two-thirds said their organization had been affected by malware or viruses downloaded by employees and the majority acknowledged they were fully aware of the risks of unmonitored and uncontrolled Internet use.

Key findings:

- 69.9% say they use a web filtering / web security solution to control and monitor Internet use in their organization
- 65.4% of those who do NOT have a web filtering or web security solution experienced a malware or virus attack via downloaded files
- 85% of those who use web filtering/security solutions allow employees to surf the Internet for personal reasons during office hours
- 80% of respondents have an Acceptable Use Policy on Internet usage
- 92.5% inform their employees that their online activity may be monitored.

Methodology

The survey was conducted among small and medium-sized businesses with a total of 631 respondents. The survey population was compiled from a list of those who visited http://www.gfi.com and downloaded a trial but are NOT customers OR Partners of GFI Software.

Demographics

The majority of respondents are in IT management or IT staff working in network management and administration and work in a range of industries. A total of 17.5% and 13.5% work in the financial sector and in computer services/ consulting respectively. In terms of company size, 63.9% of SMEs had between 1 and 99 employees. Only 8.9% or 56 SMEs had over 500 employees.

GFI Software
Magna House, 18-32 London Road, Staines, Middlesex TW18 4BP, UK
tel: +44 (0) 870 770 5370 | fax: +44 (0) 870 770 5377
email: sales@gfi.com | url: www.gfi.com