MarketVibe

July 2008

Online Security Issues in Regulated Industries

Research conducted by:

COMPUTERWORLD

Sponsored by:

Contents

Online Security Issues in Regulated Industries

Overview

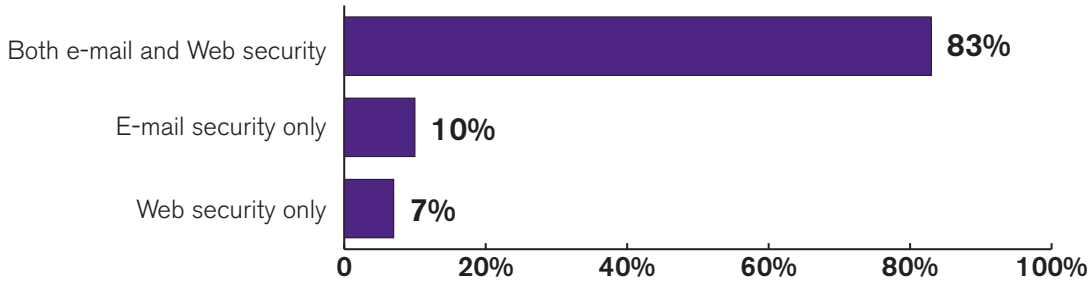
In June 2008, *Computerworld* invited IT and business leaders to participate in a survey on online security initiatives at their organizations. The survey was fielded via targeted broadcasts to *Computerworld* customers, as well as through an invitation on *Computerworld.com*. The goal of the survey was to better understand Web and e-mail security issues faced today within the regulated education, financial services, government and health care industries. The following report represents top-line results of that survey.

Profile of respondents

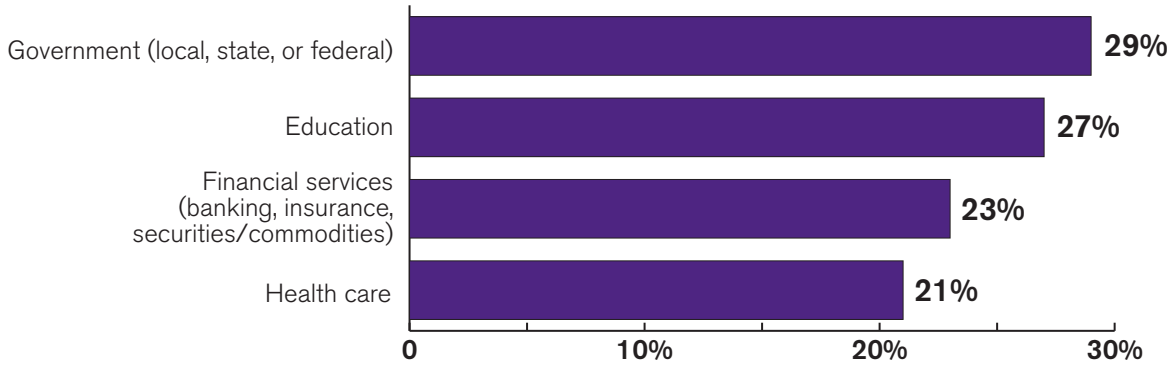
Total respondents: 103

All 103 respondents were qualified through a series of screening questions as being involved in IT security purchase decisions at organizations with 50 or more computers. Additionally, respondents were required to have most of their organization's computers be Windows-based and had to be in one of the following industries: education, financial services, government or health care. The following chart provides a breakdown of respondents' involvement with the purchase decisions for IT security products at their organizations. This chart is followed by a breakdown of respondents by industry, number of computers, full-time employees in the IT department, and job title.

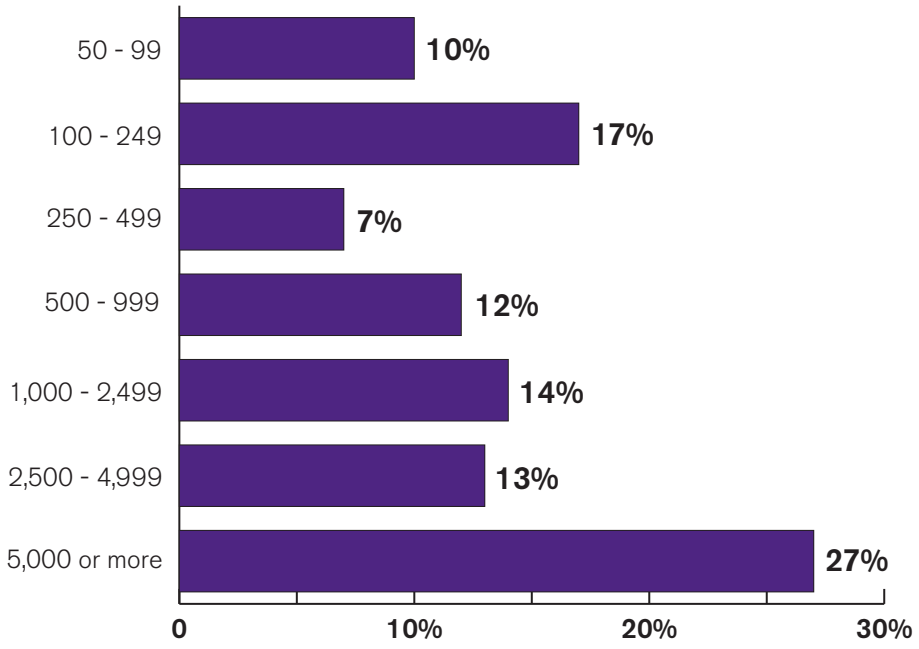
For which of the following solutions do you make IT security purchase decisions for your organization?



What is your organization's primary industry?

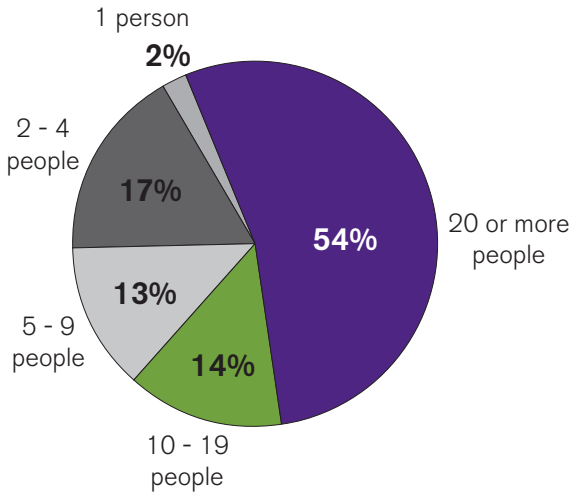


Approximately how many computers (PCs and laptops) do you have in your organization?



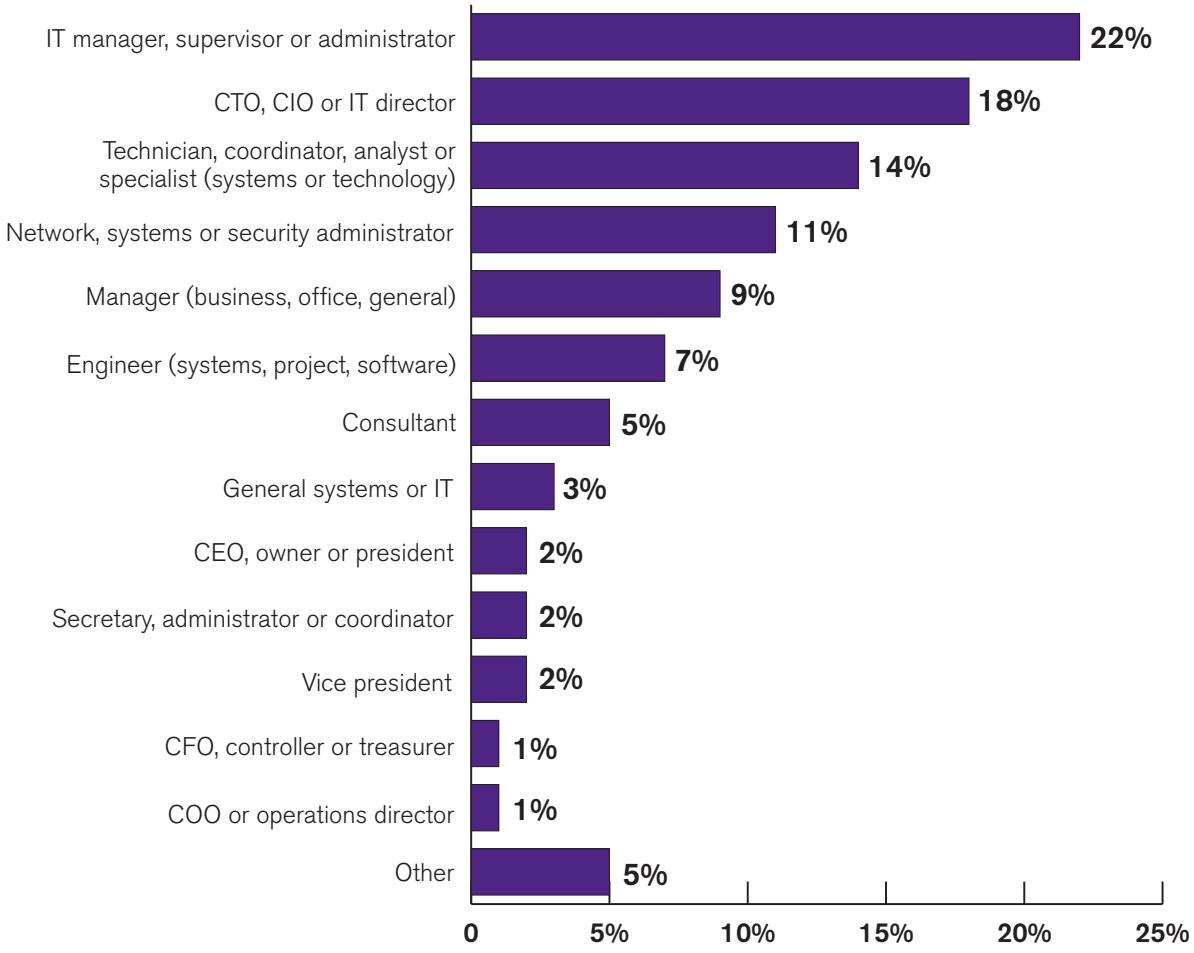
Average number of computers: 2,364

How many people work full-time in your organization's IT department?



Average number of full-time IT employees: 17

Which of the following most closely matches your title?



Note: Percentages don't add up to 100 because of rounding.

Executive summary

Every year, it becomes harder to protect virtual environments from potential internal or external threats to data and confidential information. Organizations are continually working to keep up with the changing environment of the Internet in order to protect their most valuable data from exposure. The results from this study show that Web and e-mail security are critical to organizations, with serious online threats affecting many areas of the organization.

Organizations are more concerned about infections from viruses and spyware than they are about any other threat. More than eight out of 10 respondents are extremely or very concerned about these threats. Other top concerns include data breaches resulting in lost customer data and ensuring e-mail confidentiality.

Not surprisingly, the problems most often plaguing respondents over the last 12 months included spyware and viruses or worms. These two problems have impacted nearly two-thirds of all respondents. While the incidence of other problems such as security breaches, unintentional release of private customer information and loss of intellectual property is lower, these are serious issues impacting respondent organizations.

E-mail- and Web-based threats are impacting respondent organizations in many ways, with the most significant being a decrease in network speed, an increase in help desk time to repair damage to computers, and a negative impact on server performance. Security and compliance requirements for organizations in regulated industries are especially challenging, with more than four out of 10 respondents required to comply with HIPAA regulations, and 20% or more required to comply with the Sarbanes-Oxley Act, the PCI Standard and the Gramm-Leach-Bliley Act.

It is also clear from this study that keeping Web and e-mail security protection up to date is challenging for organizations and that more resources need to be devoted to this area. In fact, more than eight out of 10 respondents report that keeping Web and e-mail security protection up to date is challenging. Additionally, just over half of all respondents strongly or somewhat agree that their organizations devote insufficient resources to Web and e-mail security.

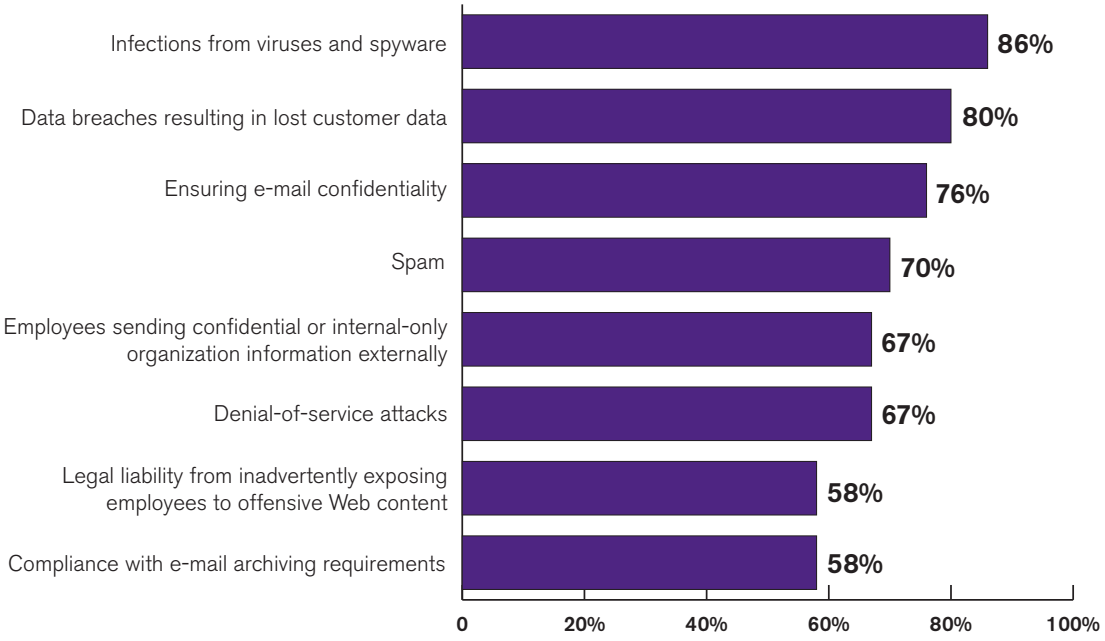
Organizations rely on e-mail and the Web for many business tasks. In fact, more than eight out of 10 respondents rate e-mail and the Web as extremely or very important to communication and collaboration among employees and partners. Other important tasks include communicating with customers and accessing Web-based applications.

To aid in the prevention of data leakage and security breaches many organizations are implementing security strategies and policies. Most notably, more than three quarters of respondents report that they are currently using or planning to implement Web/URL filtering to restrict access to inappropriate Web sites. More than seven out of 10 respondents have also implemented or plan to implement e-mail security software as a service as part of their security strategy.

E-mail and Web security issues

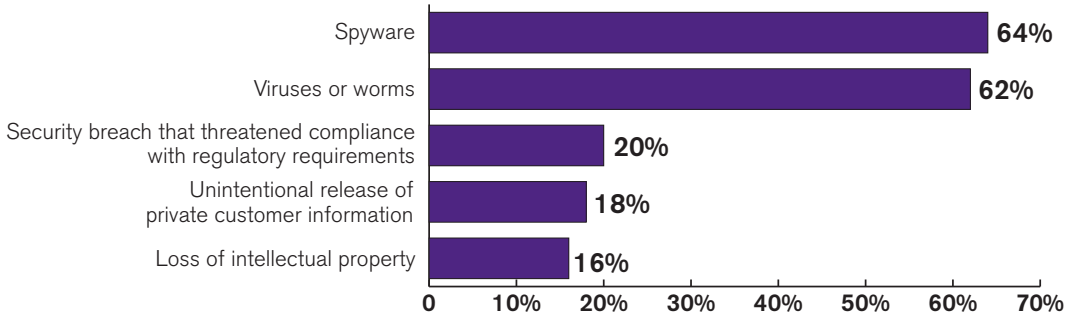
E-mail and Web security issues are pressing concerns for organizations. When asked which e-mail and Web security issues they are most concerned about, 86% said they are extremely or very concerned about infections from viruses and spyware. Other top e-mail and Web concerns include data breaches resulting in lost customer data and ensuring e-mail confidentiality.

Percentage of respondents answering 'extremely' or 'very' concerned



Problems experienced via e-mail or the Web in the past 12 months

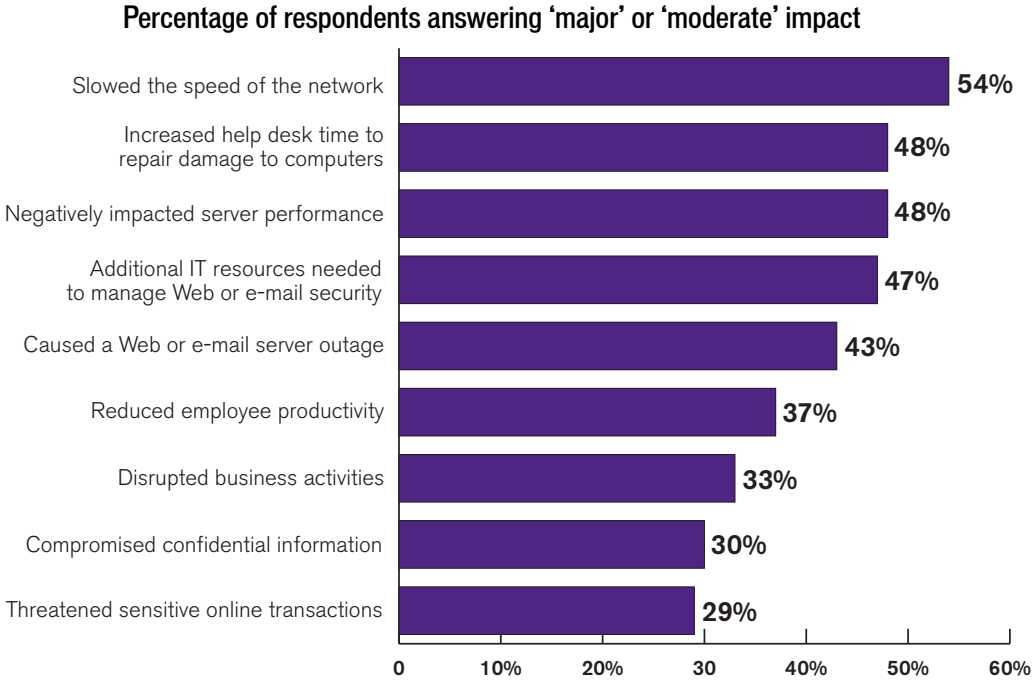
The most common problems experienced via e-mail or the Web are spyware and viruses or worms, which have affected nearly two-thirds of all respondents. While the incidence of other problems – such as security breaches, unintentional release of private customer information and loss of intellectual property – is lower, these are also serious issues impacting respondent organizations.



Multiple responses allowed.

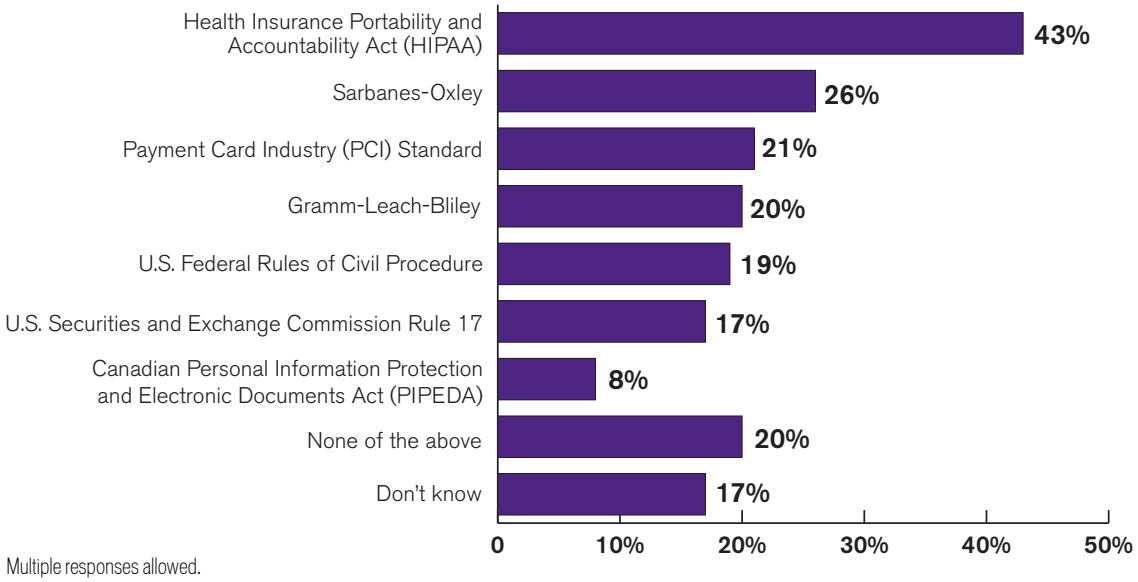
Areas impacted by e-mail- and Web-based threats in the past 12 months

E-mail- and Web-based threats are impacting respondent organizations in many ways, with the most significant being a decrease in network speed, an increase in help desk time to repair damage to computers, and a negative impact on server performance.



Compliance regulations

The need to comply with various regulations is high, with more than four out of 10 respondents (43%) required to comply with HIPAA regulations specifically. Other regulations respondent organizations are required to comply with include the Sarbanes-Oxley Act (26%), the PCI Standard (21%) and the Gramm-Leach-Bliley Act (20%). Only 20% of respondents are not required to comply with any of the regulations listed below.

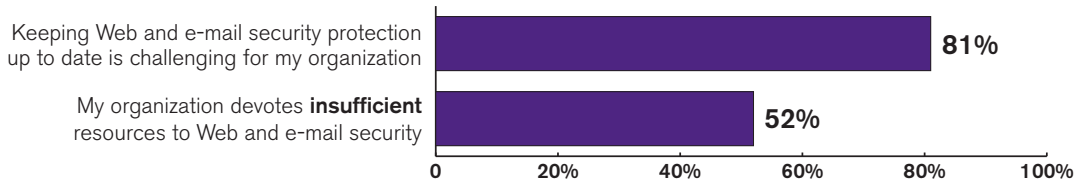


Multiple responses allowed.

Agreement with statements regarding e-mail and Web security

When asked their level of agreement with various statements regarding e-mail and Web security, more than eight out of 10 respondents (81%) report that keeping Web and e-mail security protection up to date is challenging for their organizations. While agreement with the statement regarding organizations devoting insufficient resources to Web and e-mail security is lower, more than half of respondents (52%) agree with it.

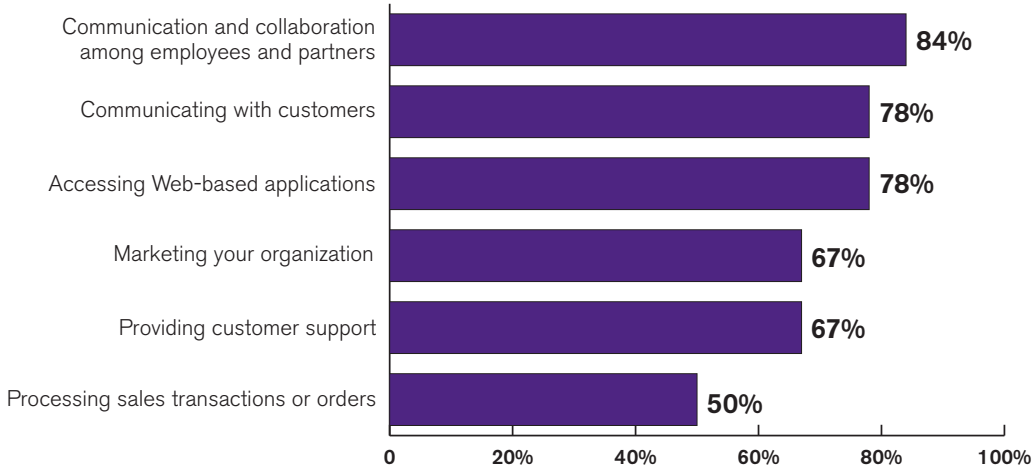
Percentage of respondents answering 'strongly' or 'somewhat' agree



Importance of e-mail and the Web for performing business tasks

It is clear that e-mail and the Web are important for performing business tasks at respondent organizations, with more than eight out of 10 respondents (84%) indicating that e-mail and the Web are extremely or very important for communication and collaboration among employees and partners. Additionally, more than three-quarters of respondents (78%) rate e-mail and the Web as extremely or very important for communicating with customers and accessing Web-based applications.

Percentage of respondents answering 'extremely' or 'very' important

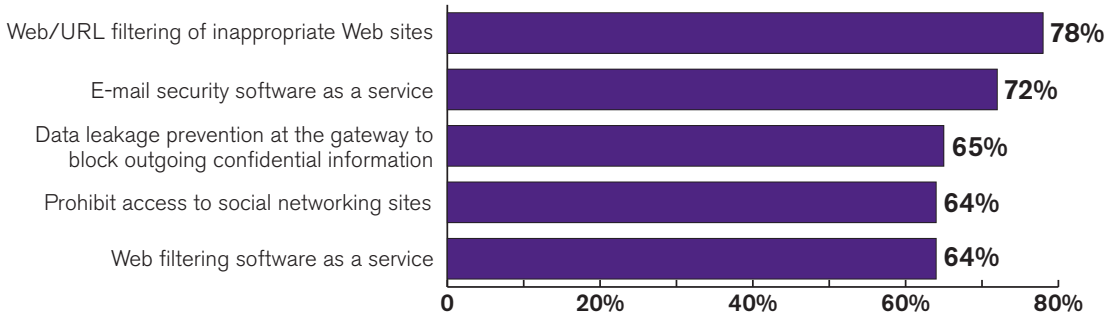


Security strategies and policies at respondent organizations

While half of all respondents (50%) indicate that their organizations use one or more Web 2.0 applications, such as social networking, wikis or blogs, organizations are currently implementing or planning to implement various security strategies and policies related to the Web.

In fact, over three quarters of respondent organizations (78%) have implemented or plan to implement a Web/URL filtering of inappropriate Web sites as a part of their security strategy or policy. Meanwhile 72% have or plan to implement e-mail security software as a service, and 65% have or plan to implement data leakage prevention at the gateway to block outgoing confidential information.

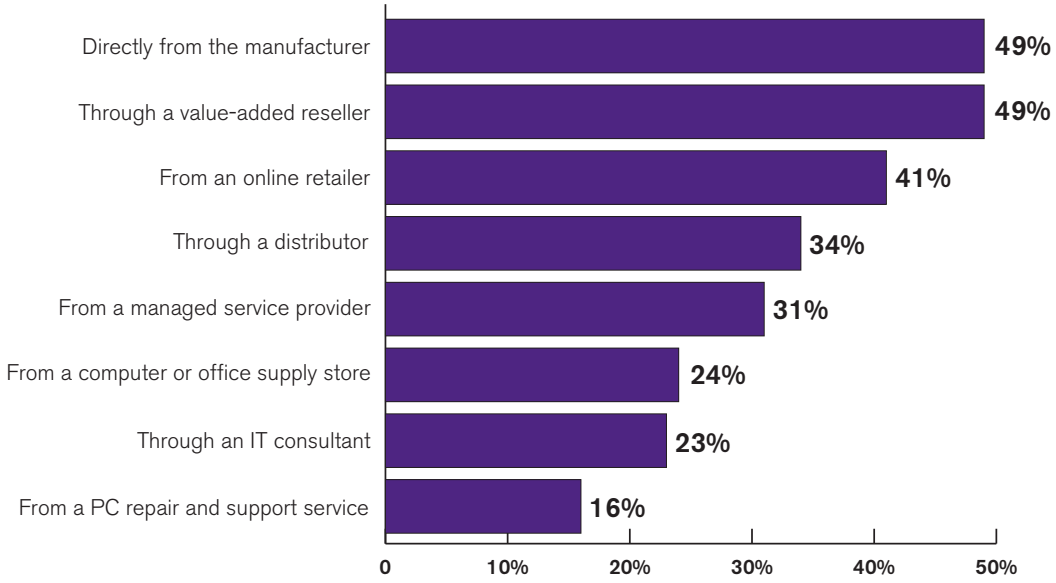
Percentage of respondents answering 'implemented' or 'plan to implement'



Frequency of purchasing security solutions through various sources

When respondents were asked how often they purchase security solutions from various sources, it could be seen that they most frequently purchase directly from the manufacturer or through value-added resellers with nearly half of all respondents (49%) purchasing from one of those sources most of the time or often. Other top security solution sources purchased from most of the time or often include online retailers (41%), distributors (34%) and managed service providers (31%).

Percentage of respondents answering 'most of the time' or 'often'



Conclusion

It is clear that Web and e-mail security is critical to organizations whose top concerns include infections from viruses and spyware, data breaches resulting in lost customer data and ensuring e-mail confidentiality. Organizations are facing serious online threats with spyware and viruses or worms being the most common. In addition, roughly two out of 10 respondents said they had been impacted by security breaches that have threatened compliance with regulatory requirements, unintentional release of private customer information and loss of intellectual property.

E-mail and Web-based threats are negatively affecting organizations' network speed and server performance, and they are forcing organizations to increase IT resources to repair damaged computers and to manage Web and e-mail security. E-mail and the Web are critical in performing business tasks, especially related to communication among employees, partners and customers.

Since keeping Web and e-mail security protection up to date is a major challenge, the adoption of security strategies such as e-mail security software as a service and Web filtering software as a service can help organizations by delivering a manageable solution that offers better protection against viruses, spyware and other online threats.