White Paper

How Organizations Are Managing Their Firewall Infrastructure

Research conducted by: COMPUTERWORLD
The Voice of IT Management

July 2007

Sponsored by: AlgoSec

Contents

Overview . . . 3

Profile of respondents . . . 3

Executive summary . . . 6

Frequency of auditing firewall configurations . . . 7

Approximate length of time between a firewall rule change request and its implementation . . . 7

Level of concern regarding potential security holes in a company's firewall . . . 8

Importance of having a solution that automates the firewall audit process . . . 8

Importance of firewall infrastructure issues . . . 9

Need to search/query to identify redundant and unused rules and/or objects in firewall configurations . . . 9

Frequency of changing the IP address of business critical servers . . . 10

Importance of ensuring operational traffic is not blocked when changing the IP addresses of important servers . . . 10

Compliance requirements necessitating the use of the company firewall . . . 11

Expected 2007 expenditures for firewall management solutions . . . 12

Conclusion . . . 12

How Organizations Are Managing Their Firewall Infrastructure

Overview

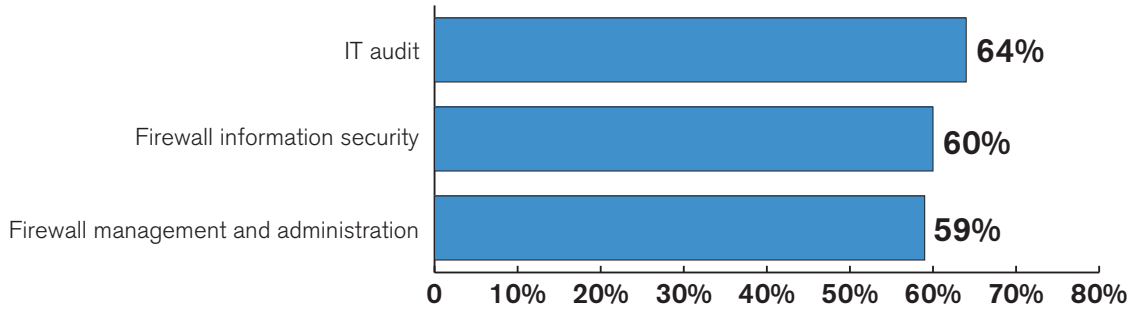
In May/June 2007, *Computerworld* invited leaders in IT audit, firewall information security, and firewall management and administration at companies with a minimum of three firewalls/firewall clusters and up to thousands of firewalls/firewall clusters to participate in a survey on firewall audit and management. 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 the firewall audit and management process and the security concerns of organizations today. The survey was commissioned by AlgoSec, but data was gathered and tabulated independently by Computerworld Research. The following report represents top-line results of that survey and is meant to serve as a brief benchmarking tool for leaders seeking information about how their peers are addressing firewall audit and management within their organizations.

Profile of respondents

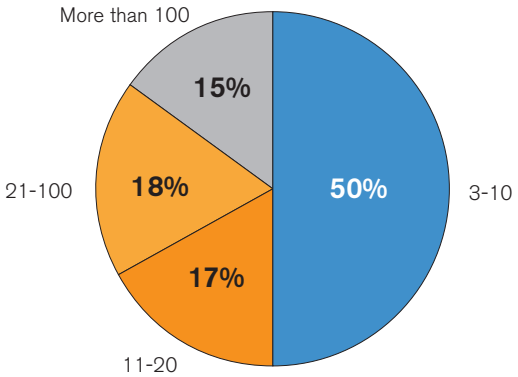
Total Respondents: 206

All 206 respondents were qualified through a series of screening questions and are responsible for IT audit, firewall information security or firewall management and administration at their organizations. The chart below is a breakdown of the percentage of respondents by involvement. The following pages show the breakdowns of the respondents based on the number of firewalls/firewall clusters, job title, annual revenues, industry and location.

Are you responsible for any of these technology issues in your company?

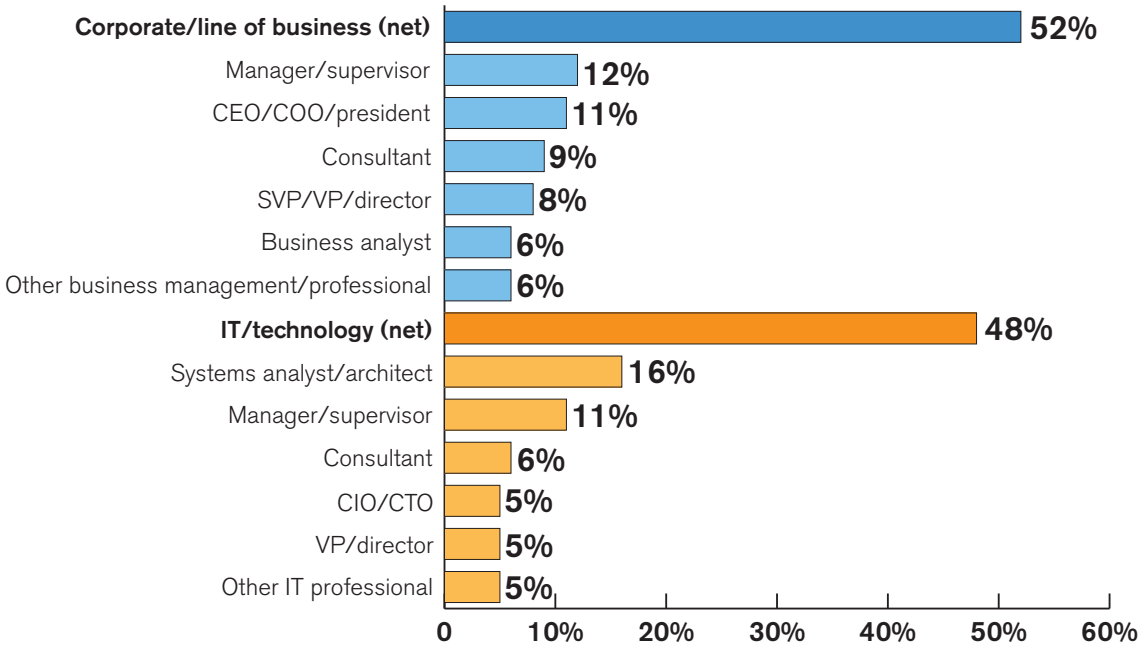


How many firewalls/firewall clusters are in your company's network?

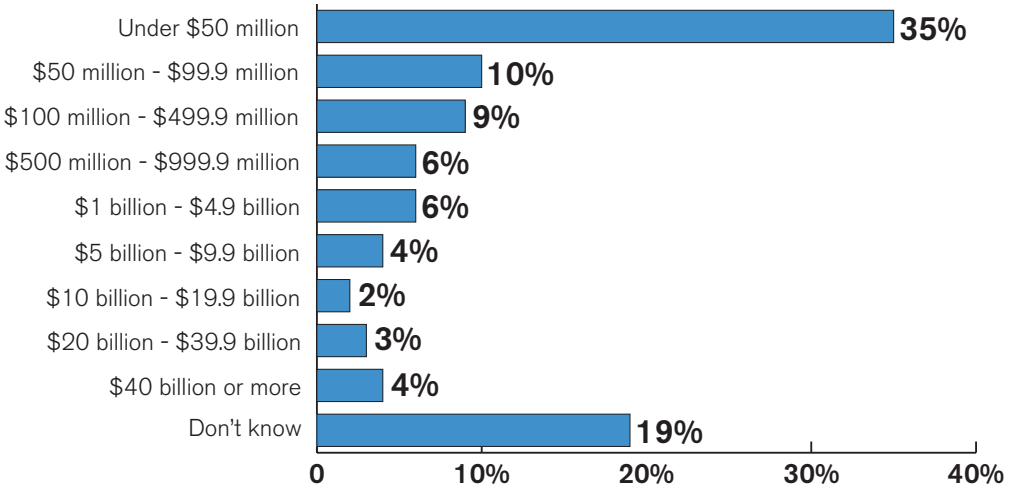


Average: 32 firewalls/firewall clusters

Which of the following best describes your job title/function?

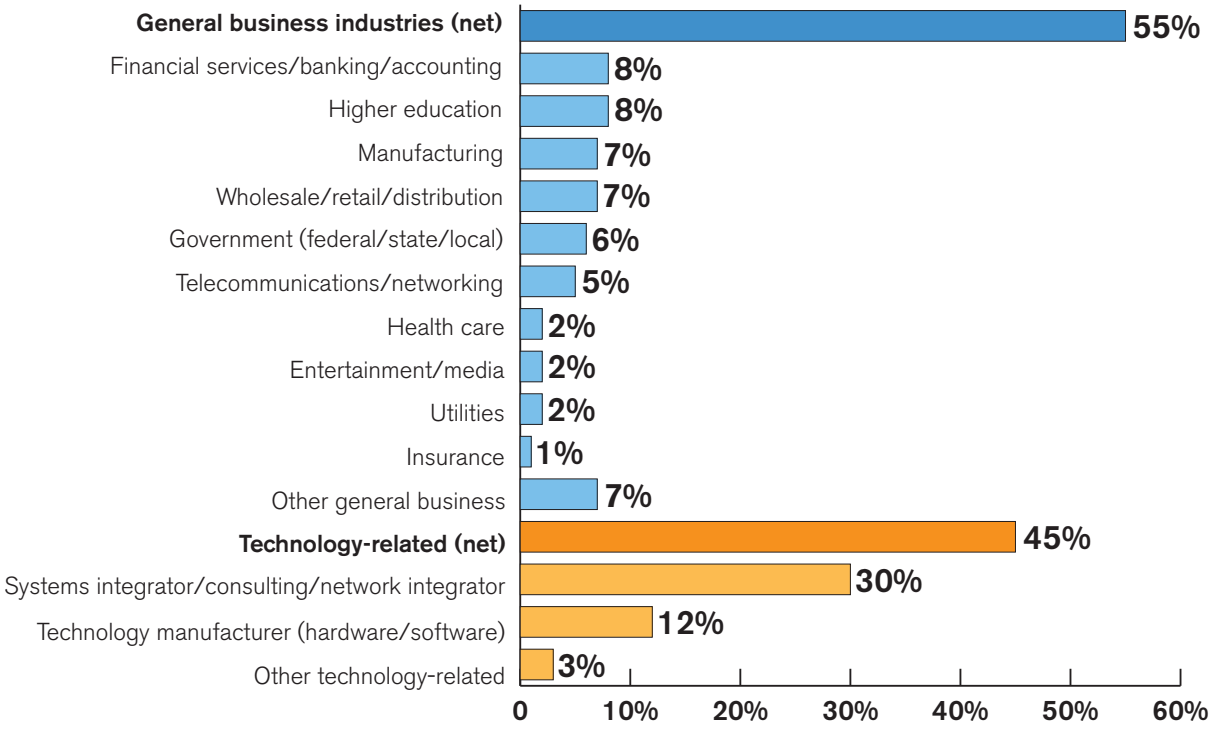


What are your company's estimated 2007 gross annual revenue?

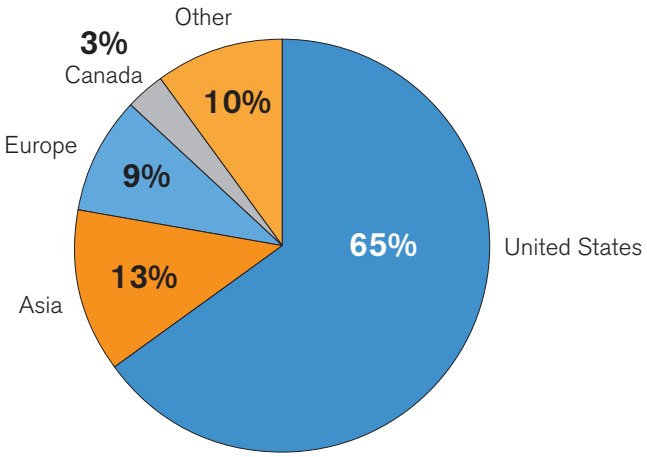


Average: $4.6 billion

What is your company's primary business or industry?



Where is your organization/company located?



Executive summary

This survey was conducted to better understand the firewall audit and management process and the security concerns of organizations today. Several interesting conclusions emerged from the feedback provided by the respondents. The first, is the importance of having a solution that automates the firewall audit process. Two-thirds of respondents (67%) found it critical or important that a solution be put into place to automate the firewall audit process. This may be driven by the fact that nearly three quarters of respondents (73%) are concerned about potential security holes in their company's firewall configurations.

While a large percentage of respondents are concerned about potential security holes and rate the importance of having a solution that automates the firewall audit process as high, only 27% of respondent companies currently audit their firewall configurations on a weekly basis. This could be an upcoming area of focus for organizations since two-thirds rated the issue of audits as critical or important to their company's firewall infrastructure.

Another issue exposed by this survey is the fact that 58% of respondents reported that their company needs to search/query to identify redundant and unused rules and/or objects in its firewall configuration but do not have the ability. With the ability to easily search/query their firewall infrastructure, organizations would be able to work efficiently and easily manage their firewalls and their firewall rule sets. Additionally, being able to optimize policy relative to their company's firewall infrastructure is considered critical or important to roughly two-thirds of the respondents.

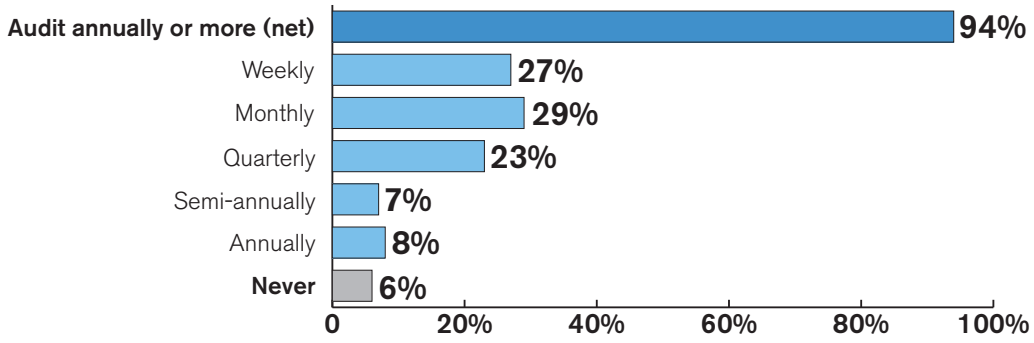
With today's constant demand for application and infrastructure changes, there is a significant risk of compromising security in the process and creating inefficiencies. We see in this research that nearly seven out of 10 respondents (69%) have at some point changed the IP addresses of business critical servers. The importance of ensuring that operational traffic is not blocked when changing the IP addresses of important servers is critical to nearly half (46%) of respondents. Additionally, three quarters of respondents rated change management as critical or important to their company's firewall infrastructure.

Lastly, with over two-thirds of respondents having compliance requirements necessitating the use of the company's firewall, including Sarbanes-Oxley (45%), ISO 17799 (37%) and HIPAA (35%), organizations need to be able to view all the risks and the specific rules that are causing them across all their firewalls. More than eight out of 10 respondents rated risk management (85%) and security compliance (82%) as critical or important to their company's firewall infrastructure.

Frequency of auditing firewall configurations

While virtually all respondent companies (94%) audit their firewall configurations to some extent, only 27% audit them on a weekly basis. Roughly three out of 10 respondents report a monthly audit, while 22% indicate that a quarterly audit typically takes place at their company.

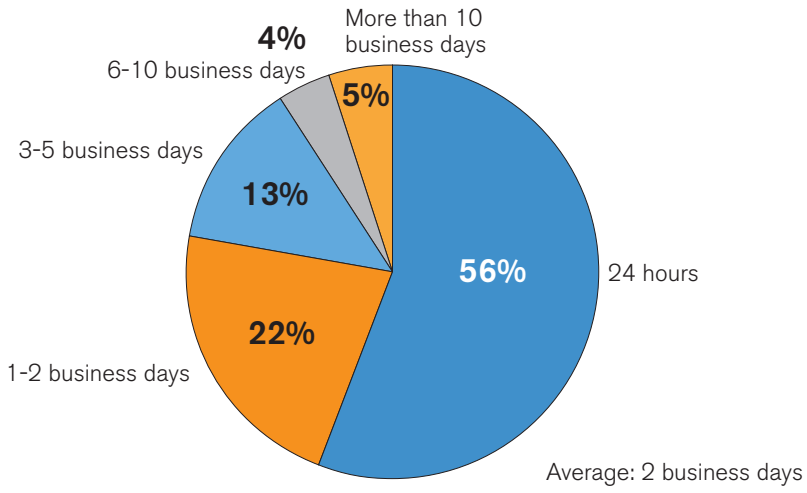
How often does your company typically audit its firewall configuration?



Approximate length of time between a firewall rule change request and its implementation

Among respondents whose companies audit their firewall configurations at least annually, it typically takes two business days between a firewall rule change request and its implementation. Fifty-six percent of respondents reported that it typically takes 24 hours between a firewall rule change request and its implementation.

How long does it typically take between a firewall rule change request and its implementation?

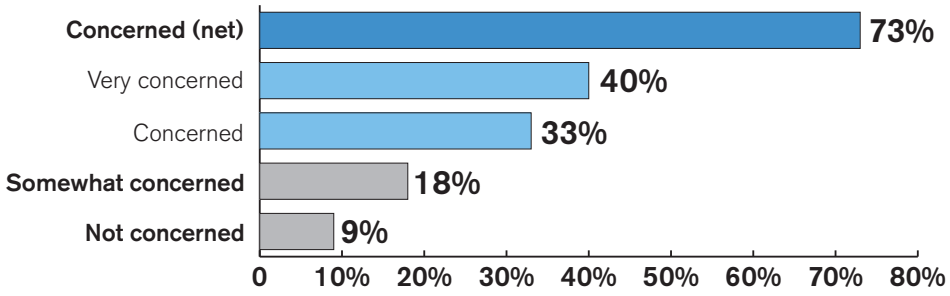


Overall base: 193 respondents whose company audits its firewall configuration

Level of concern regarding potential security holes in a company's firewall

While only slightly more than one quarter of respondents (27%) typically audit their firewall configurations on a weekly basis, 73% of respondents are concerned about potential security holes in their company's firewall. More specifically, 40% of respondents are very concerned about potential security holes. It appears that many organizations have not yet taken the step toward making an investment in the area of automated audits, and manual audits can be time consuming and error prone.

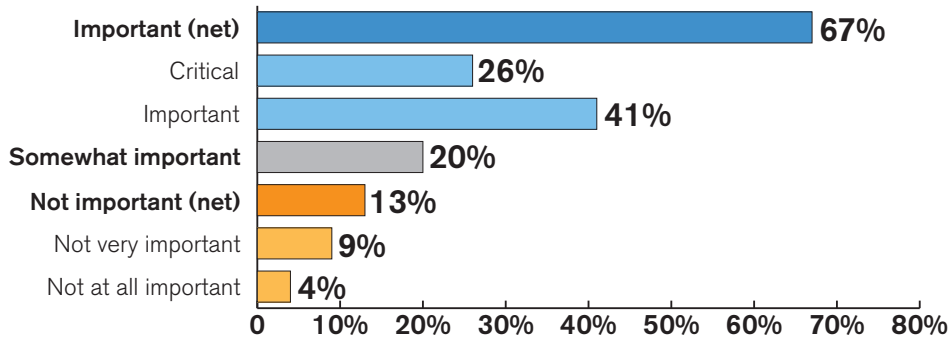
How concerned are you about potential security holes in your company's firewall?



Importance of having a solution that automates the firewall audit process

As reported earlier, while virtually all respondent companies (94%) audit their firewall configurations to some extent, only 27% audit them on a weekly basis. However, respondents place a high level of importance on having a solution that automates the firewall audit process. In fact, more than one quarter of respondents (26%) considered it critical that a solution be put into place to automate the firewall audit process. Two thirds of respondents (67%) found it important to have this type of solution.

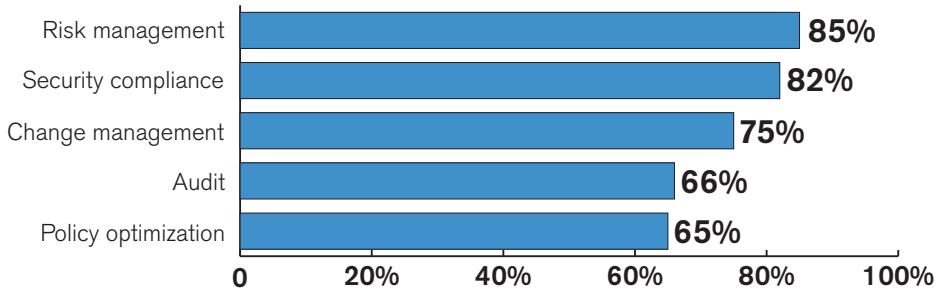
How important is it to you to have a solution that automates the firewall audit process?



Importance of firewall infrastructure issues

Approximately two-thirds of respondents or more rated each of the firewall infrastructure issues as critical or important. In fact, 85% of respondents rated risk management as critical or important relative to their company's firewall infrastructure.

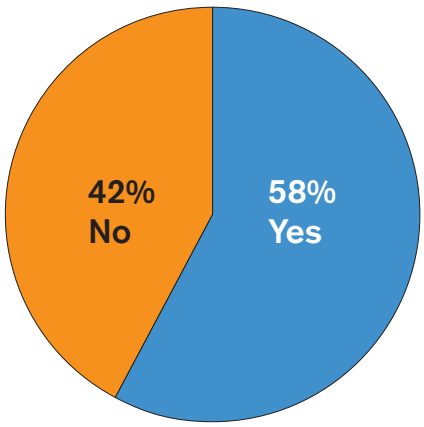
On a scale of 1 to 5, with 1 being not at all important and 5 being critical, please rate how important each of the following issues are relative to your company's firewall infrastructure. Respondents answering "critical" (5) or "important" (4):



Need to search/query to identify redundant and unused rules and/or objects in firewall configurations

Nearly six out of 10 respondents (58%) reported that their company would like to have the ability to search/query to identify redundant and unused rules and/or objects in its firewall configuration. With this approach, organizations would be able to work efficiently and easily manage their firewalls.

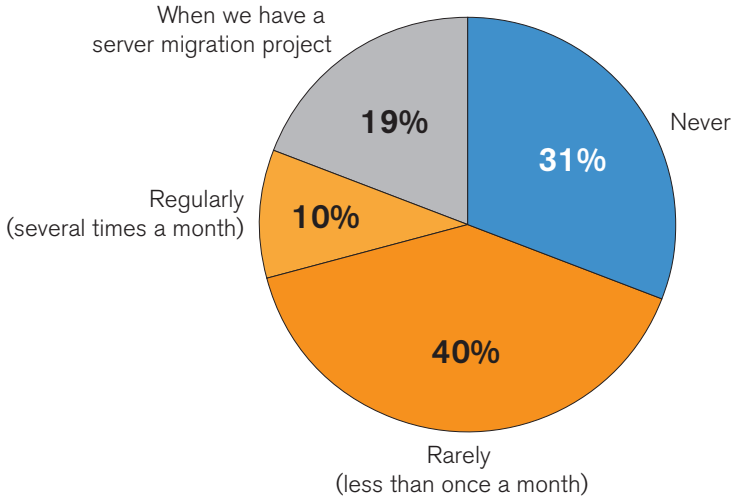
Does your company need to search/query to identify redundant and unused rules and/or objects in its firewall configuration?



Frequency of changing the IP address of business critical servers

Nearly seven out of 10 respondents (69%) report that they have at some point changed the IP address of business critical servers. More specifically, 19% have changed the IP address when they have a server migration project, while 10% change the IP address of business critical servers regularly (several times a month).

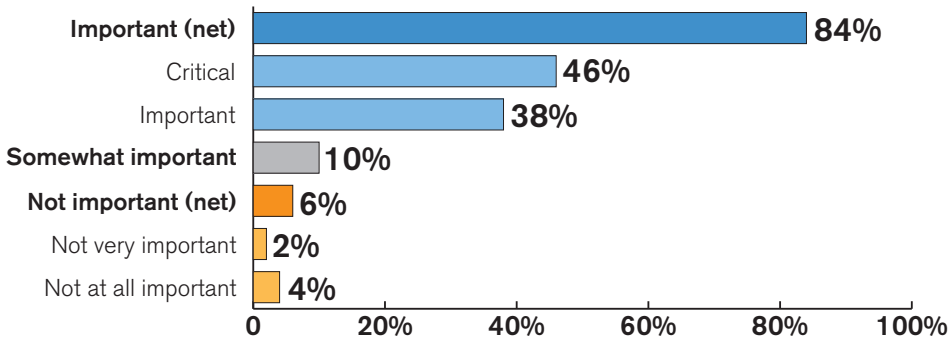
How often does your company typically change the IP address of business critical servers?



Importance of ensuring operational traffic is not blocked when changing the IP addresses of important servers

Importance of ensuring that operational traffic is not blocked when changing the IP addresses of important servers is important to most respondents (84%) while 46% rated this as a critical issue. Forty-four percent of respondents reported that it is difficult to locate the exact objects in their firewall that need to be updated to ensure continuity and avoid disruptions to their operations.

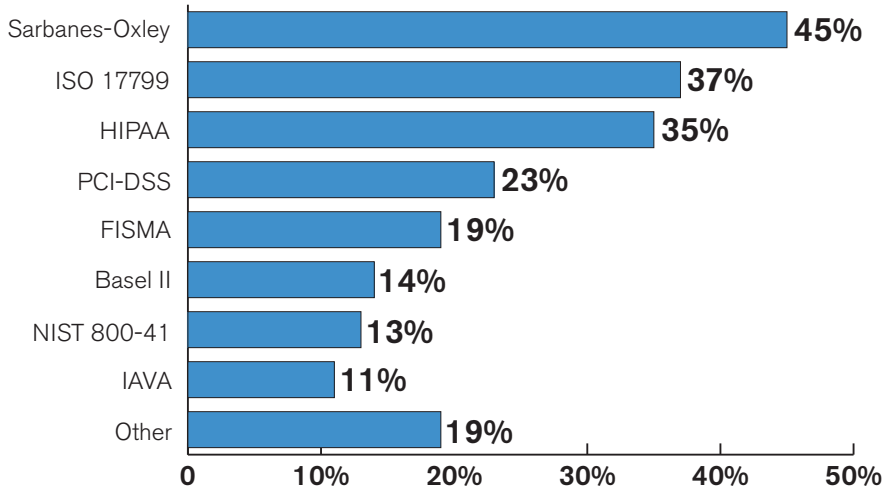
How important is it to ensure operational traffic is not blocked when changing the IP addresses of important servers?



Compliance requirements necessitating the use of the company firewall

Just over two-thirds of respondents (68%) have compliance requirements necessitating the use of their company's firewall. Among these respondents, the most common compliance requirements are Sarbanes-Oxley (45%), ISO 17799 (37%) and HIPAA (35%).

Please identify which compliance requirements necessitate your company's use of the firewall.

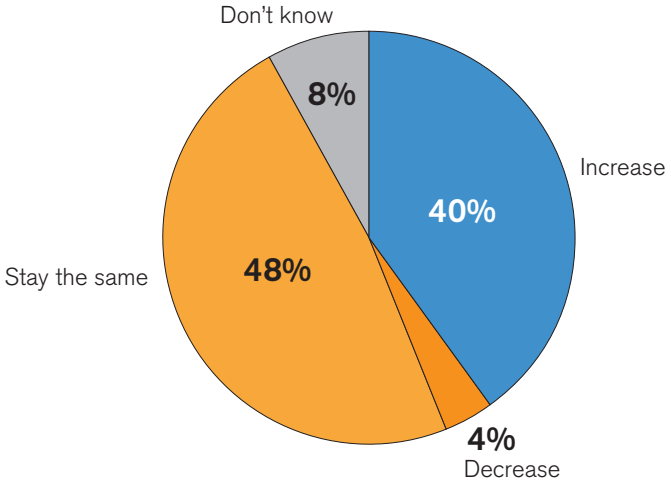


Overall base: 140 respondents with compliance requirements necessitating the use of the company firewall

Expected 2007 expenditures for firewall management solutions

It is not surprising based on the high level of concern about potential security holes in their company's firewall and the high level of importance on having a solution that automates the firewall audit process that overall, 88% of respondents reported that their firewall management solution expenditures will increase or remain the same in 2007. More specifically, 40% of respondents indicated that their company's 2007 expenditures for firewall management solutions will actually increase over 2006.

For 2007, will your company's expenditures for firewall management solutions increase, decrease or stay the same as 2006?



Conclusion

The level of concern about potential security holes in their company's firewall configurations and the importance of ensuring that operational traffic is not blocked when changing the IP addresses of important servers, makes it clear that organizations today need to increase their level of investment in firewall management solutions to detect risks and decrease threats to the organization's security and to prevent any impact on the bottom line.

So what does all this mean for your organization? Basically, your organization can use responses from this survey as a benchmark for how your peers are addressing these issues. If your organization is not currently utilizing or investigating firewall management solutions, you need to begin to address this critical issue. It's important that the solution you seek is comprehensive and that it enables your organization to alert you about events that may happen in the future so you can practice prevention instead of crisis management.