

November 2, 2007

Commissioned by



Top Line Summary

In September 2007, Cisco commissioned the e-gov institute to conduct a web-based survey of federal IT decision-makers. Respondents were asked about their main security efforts and issues and progress and concerns with federal initiatives. Respondents from more than 30 federal agencies were represented in the study.

I. Security Trends (2005-2007)

The security survey has been conducted annually for the past three years (2005-2007). After reviewing the data from each year, the following conclusions were made:

- Importance of security issues has remained relatively constant. Network firewalls, network intrusion detection, and server and workstation security have been of top importance each year.
- Respondents were more concerned in general with various security issues and threats in 2007 than in previous years. Security breach issues, such as reduced operations and loss of privacy of data, were respondents' top concerns in all three years.
- Time spent on security is not decreasing. In 2006 and 2007, respondents were asked about their time spent on mandated security requirements. More than 60% in each survey said they spent more time on mandated security requirements than in the previous year.
- Level of confidence in agency security is not increasing. Respondents in 2006 and 2007 were asked about their level of confidence in their agency's security relative to three years ago. Though nearly 60% of respondents in 2006 felt more confident in their agency's security than they did three years ago, this number decreased in 2007.
- Though funding is consistently the most significant barrier in agencies' network security success, amount of required end-user training has become increasingly more important since 2005. More than half of respondents in 2007 said end-user training is a significant barrier to their agency's network security success, up from 36% in 2005.
- Attention to FISMA hit its peak in 2006. Achieving FISMA compliance, achieving green status in all categories of the PMA, and improving GAO FISMA scorecard grades were all higher priorities to respondents in 2006 than in 2005 or 2007.

II. Demographics (2007)

- 202 federal decision-makers participated in the survey. The distribution of civilian and defense respondents generally followed the overall federal spending and employment in these areas. Civilian respondents represented 56% of the sample, while defense represented 44%.
- There was an even split between business-oriented and IT-oriented respondents.
- All respondents had some involvement in network security activities, ranging from applications or data security to risk management.

III. Security Efforts and Issues (2007)

- Network level security issues were of top importance. Nine of every ten respondents considered network firewalls, network intrusion detection, and network access control to be important to their agency's total security efforts. Other more user-based security issues, such as remote access, rated slightly lower.



- Respondents reported worrying most about one-time security issues, such as reduced operations and service delivery and loss of privacy of data due to security breaches, rather than ongoing threats, such as security concerns associated with remote access and unknown application software/operating system security flaws.
- Consistent with previous years, nearly two-thirds of respondents reported spending more time on mandated security requirements than they did one year ago.
- Approximately half of respondents said they felt more at ease with their agency's security than they did three years ago.
 - Defense respondents were generally less at ease than civilian respondents.
- Funding was the most significant barrier to improving respondents' agencies' network security capabilities. Amount of required end-user training has become a top level barrier to success since 2005.
- Half of respondents encountered a lack of collaboration among stand-alone products within their existing security architecture.
 - IT respondents, specifically, encountered a lack of integrated reporting.

IV. Federal Initiatives and Requirements (2007)

- Civilian respondents generally placed a higher priority on all federal initiatives than defense respondents.
- Approximately 70% of respondents had at least some level of awareness of their agency's efforts to achieve FISMA compliance. Nearly 30% were aware of and involved in their agency's efforts to become compliant.
 - IT respondents were more likely to be aware of and involved in FISMA compliance than business respondents.
- Nearly half of respondents reported committing more than 25% of their time to achieve FISMA compliance.
 - Civilian respondents spent less time on compliance than defense.
- Funding was cited by one-third of respondents as a top challenge in achieving overall FISMA compliance. One-quarter cited management awareness and support as a challenge.
 - IT respondents were more likely than business respondents to consider the ability to enforce security policy as a top challenge.
- More than one-third of respondents said their agency is developing or has developed an IPv6 security architecture.
- Nearly 60% of respondents indicated that they expect IPv6 to improve their agency's security posture.

V. Security Impact of Web 2.0 (2007)

- More than 40% of respondents considered the security impact of allowing Web 2.0 functions on their networks to be a high priority concern.
- Respondents most often mentioned social networking, file sharing, remote access, and application compatibility as their agency's greatest Web 2.0-related security concerns.