

Information Security Awareness Report[™]

The Government Workers' Perspective[™]

May, 2007

Copyright © 2007 by SecureInfo Corporation.
All Rights Reserved.

Table of Contents

Executive Summary	3
Introduction	4
Awareness Report Findings.....	6
Methodology.....	6
Demographic Information.....	7
Survey Results	8
Conclusions.....	10
Summary.....	11
Appendix.....	12

Executive Summary

Information Security awareness is critical to assuring our nations' information assets are protected and always ready to meet mission objectives. Realizing that Information Security is as much of a people issue as it is a technology issue, the Federal government has enacted legislation (i.e., FISMA) and published standards (e.g., NIST SP800-50, DoD 8570.01 M, DCID 6/3) to ensure government workers are aware and trained on pertinent regulations, policies, and procedures. Failure to provide effective Information Security awareness training to government workers and full-time contractors puts an agency's mission at great risk and jeopardizes the economic and security interests of the United States.

SecureInfo developed the Information Security Awareness Report to provide an independent, cross-agency, quantitative analysis on the effectiveness of the Federal government's Information Security awareness training programs. By focusing exclusively on the government worker's perspective, the SecureInfo Information Security Awareness Report provides a unique and important view of the effectiveness of Information Security awareness training. Federal government workers were anonymously interviewed and asked a series of questions regarding FISMA and Information Security.

The Report found that FISMA is not widely known and its mission and purpose are often misunderstood. When known, FISMA is often viewed as a compliance headache rather than a framework for improving information security.

Protecting information assets can only be accomplished if organizations implement a sustainable information security program, of which awareness training is an essential and foundational component. However, implementing awareness training is not enough. The Information Security Awareness Report results demonstrate that awareness programs must be continually measured for effectiveness. The Information Security Awareness Report includes summary of findings; analysis of the data; methodology and demographic information on the surveyed population; and conclusions.

Introduction

The Federal government recognizes that Information Security is as much of a people issue as it is a technology issue and it has enacted legislation and published standards to ensure government workers are aware and trained on pertinent regulations, policies, and procedures. Although serious attacks from our enemies continue, a benign act by an un-aware government worker can create a significant vulnerability. The Federal Information Security Management Act (FISMA) of 2002 states that agency wide information security programs are required and shall include “security awareness training to inform personnel...who support the operations and assets of the agency of (i) information security risks associated with their activities; and (ii) their responsibilities in complying with agency policies and procedures designed to reduce these risks.”

NIST Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program*, provides guidance for building an effective information technology (IT) security program and supports requirements specified in FISMA. The publication states that, “people are one of the weakest links in attempts to secure systems and networks. The ‘people factor’...is key to providing an adequate and appropriate level of security.” The Department of Defense publication, DOD 8570.01 M, *Information Assurance Workforce Improvement Program*, requires DoD components to “provide for initial [Information Assurance] IA orientation and annual awareness training to all authorized users to ensure they know, understand, and can apply the IA requirements of their system(s).” The intelligence community’s DCID 6/3 publication stipulates that, in support of the certification and accreditation process, “the DCI shall establish and maintain a formal information security education, awareness and training program.”

Failure to provide effective Information Security awareness training to all government workers puts an agency’s mission at great risk and jeopardizes the safety and security of our entire nation.

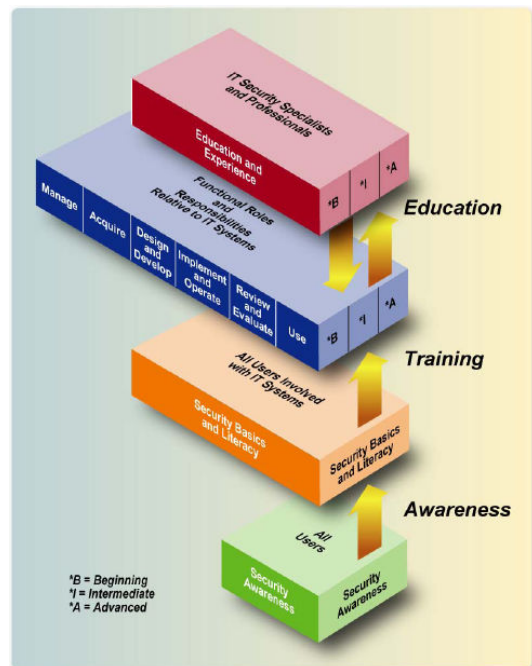
Purpose of the Information Security Awareness Report

Effective Information Security Begins with Awareness

Learning is a continuum; it starts with awareness, builds to training, and evolves into education¹.

Awareness is the foundational element and critical building block for an effective IT Security training and education program. Therefore, it is essential to measure Information Security awareness to ensure its effectiveness.

FISMA requires agency program officials, Chief Information Officers (CIOs), and Inspectors General (IGs) to conduct annual reviews of the agency's information security program and report the results to OMB. OMB uses this data to prepare an annual report to Congress on agency compliance with FISMA. The annual "*FISMA Report to Congress on the Implementation of FISMA*" is a detailed report from which the FISMA report card grades are based.



NIST SP800-50
The IT Security Learning Continuum

The FISMA report to congress includes information on the amount and percentage of government workers who have attended security awareness training but the report does not measure effectiveness of this investment. NIST SP800-50 calls for the use of metrics as a key program success indicator, but each agency is responsible for testing and measuring security awareness training.

SecureInfo developed the Information Security Awareness Report to provide an independent, cross-agency, quantitative analysis on the effectiveness of the Federal government's Information Security awareness training programs. By focusing exclusively on the government worker's perspective, the SecureInfo Information Security Awareness Report provides a unique and important view of the effectiveness of InfoSec awareness training. Numerous Information Security surveys and reports have been published focusing on the CISO's or CIO's viewpoint. While these perspectives are important for understanding priorities, concerns, and trends, the government worker's perspective is required to provide a true measure of Information Security awareness effectiveness.

Information security awareness should be designed to reinforce good security practices and change behavior as appropriate. According to NIST SP800-16, "Awareness is not training. The purpose of awareness... is to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly."

Awareness Report Findings

Background

The 2006 FISMA Report to Congress stated that there was a 10 percent increase over 2005 in security awareness training for agency employees. 3,491,290 federal employees received IT security awareness training in fiscal year 2006, which is equivalent to 91 percent of the government workforce. The total cost for providing IT security training was more than \$74 million. (See appendix for individual agency security awareness training results.)

Findings Summary

SecureInfo's Information Security Awareness Report found that there is a disconnect between the amount of government workers who attended awareness training and the effectiveness of that training. Specifically, the Awareness Report found:

1. FISMA is not widely known by government workers.
2. When known, FISMA's mission and purpose are often misunderstood.
 - FISMA is often viewed as a compliance headache, disconnected from its true purpose of improving security posture.
3. While government workers believe that their respective agencies are more secure than a year ago, the information security policies that have been implemented are negatively impacting worker productivity.

Methodology

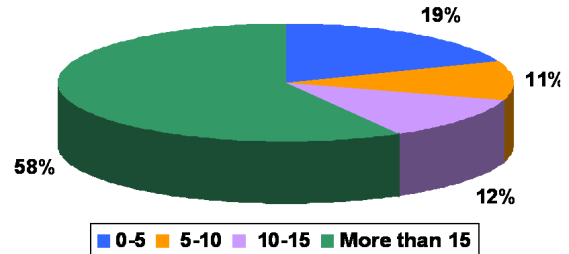
Government workers were asked to participate in an anonymous survey. Only Federal government employees and full time government contractors were included. Participants were asked a series of questions regarding FISMA and Information Security. The survey was conducted in March, 2007 after the "*FISMA Report to Congress on the Implementation of FISMA*" was published (March 1, 2007) and prior to the publication of the FISMA Report Card (April 12, 2007). Eighty five people qualified and participated in the survey.

Demographic Information

Characteristics of the surveyed government workers are included below.

Tenure in the Federal Government

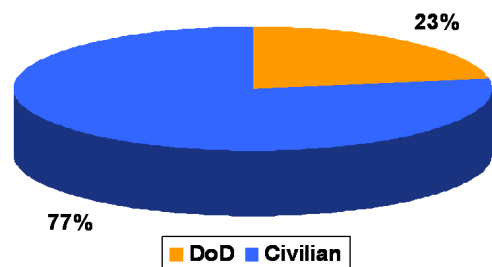
Nearly 60% (58%) have worked for the Federal government more than 15 years. More than two-thirds (70%) have worked for the government 10 years or more.



How long have you worked for the government?

Department of Defense or Civilian Agency

Approximately three quarters (77%) of participants worked for civilian agencies.



Do you work for a civilian agency or the Department of Defense?

Directly Involved in Information Security as a Job Function

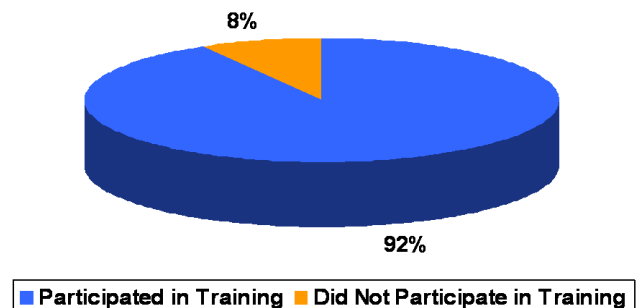
Seventy percent of participants were not involved with information security as a job function. Thirty percent of those surveyed were information security professionals.



Are you an information security professional?

Security Awareness Training

A significant majority (92%) of those surveyed participated in at least 1 security awareness training class in the past 12 months. This statistic aligns with the data reported in the 2006 FISMA Report to Congress, which reported 91% of government workers participated in security awareness training.



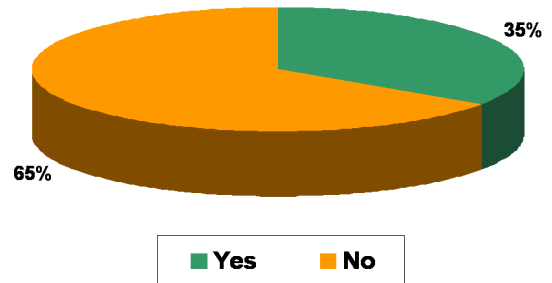
Did you participate in information security awareness training in the past 12 months?

Survey Results

Specific survey results supporting the 4 key report findings are outlined in this section.

1. *FISMA is not widely known by government workers.*

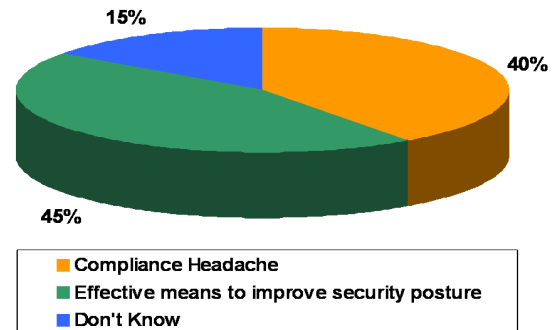
Sixty five percent of Government workers surveyed have not heard of FISMA.



Have your heard of FISMA?

2. *When known, FISMA’s mission and purpose are often misunderstood. FISMA is often viewed as a compliance headache disconnected from its true purpose of improving security posture.*

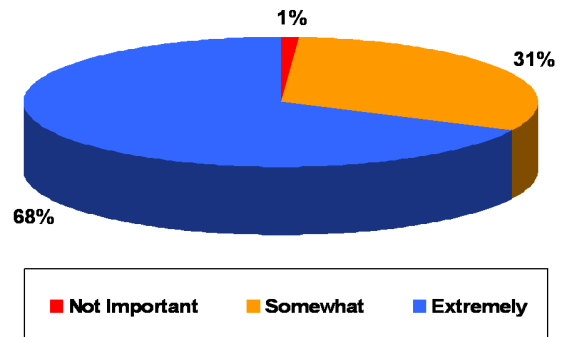
Forty percent of Government workers surveyed who have heard of FISMA believe their agency views FISMA as a compliance headache. Only 45% believe FISMA is viewed as an effective means to improve security posture.



How does your agency view FISMA?

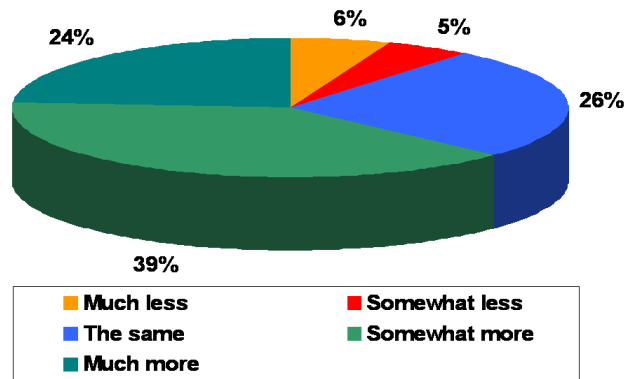
3. *While government workers believe that their respective agencies are more secure than a year ago, the information security policies that have been implemented are negatively impacting worker productivity.*

Virtually all government workers surveyed believe information security is important for achieving agency-specific goals. Two-thirds (68%) believe information security is extremely important for achieving agency-specific goals.



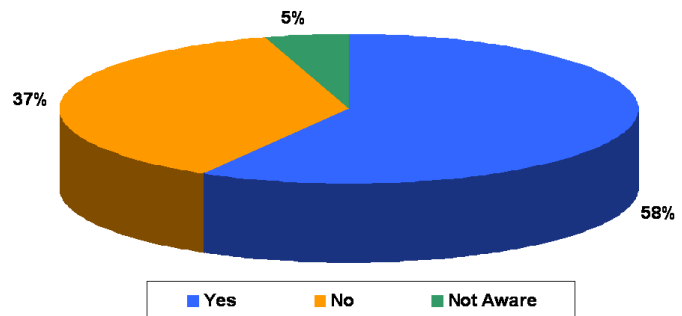
How important is information security for achieving your organization's overall business goals?

63% of Government workers believe their agency is more secure than a year ago



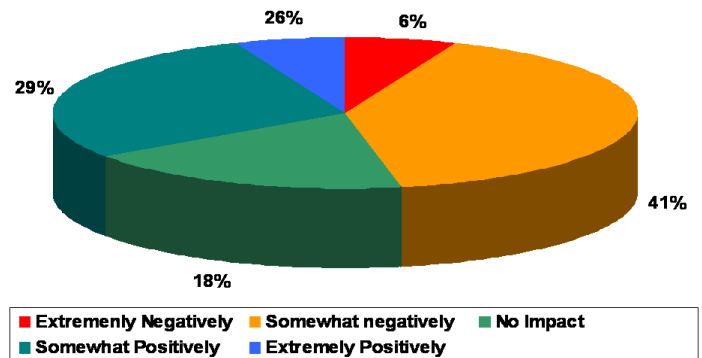
Do you think your agency is more secure today than a year ago?

More than half (58%) of Government workers believe their jobs have been affected by changes in information security policies over the past 12 months.



Has your job been affected over the past 12 months due to changes in information security policies and or/controls?

Nearly half (47%) of government workers surveyed believe their job has been negatively impacted by changes in information security policy.



Has your productivity/effectiveness been impacted by changes in security policy/or controls?

Conclusions

Information Security awareness is an essential and foundational element in assuring our nations' information assets are protected and always ready to meet mission objectives. The Federal government has enacted legislation (i.e., FISMA) and published standards (e.g., NIST SP800-50) to ensure government workers are aware and trained on pertinent regulations, policies, and procedures. However, the SecureInfo Information Security Awareness Report found that FISMA is not widely known and its mission and purpose are often misunderstood. Sixty five percent of government workers surveyed have not heard of FISMA and 40% of workers who have heard of FISMA believe their respective agencies view FISMA as a compliance headache, disconnected from its true purpose of improving security posture.

Government workers should view FISMA as a means to securing information systems rather than a “check-the-box” compliance exercise. Protecting information assets can only be accomplished if organizations implement sustainable information security program, of which awareness training is a critical and foundational component. However, implementing awareness training is not enough. Awareness programs must be continually tested for effectiveness. Recommendations to improve the effectiveness of awareness training programs are discussed below.

Measure and Report Effectiveness of Awareness Training Programs

The FISMA Report to Congress should measure and report on the effectiveness of awareness training programs. It is important to know as a baseline if government workers are receiving awareness training but the report must go beyond this to include metrics, which provide a clear indication of the effectiveness of training programs. NIST SP800-50 states that training programs should be measured for effectiveness. “Metrics monitor the accomplishment of the awareness and training program goals and objectives by quantifying the level of implementation of awareness and training and the effectiveness and efficiency of the awareness and training, analyzing the adequacy of awareness and training efforts, and identifying possible improvements.”

Include Information Security Awareness Measurement in Performance Appraisals

It is common for employees, including the government worker, to be measured on their ability to keep current with and adhere to office policies and procedures. Given the importance of information security, specific language regarding information security awareness should be inserted into all performance appraisals. Government workers, not just the agencies, should be held accountable and measured for information security awareness effectiveness.

Independently Test and Validate

Establish an ongoing program to challenge and test awareness training. This can best be accomplished by a third party to provide objective analysis of training effectiveness. The program should include random evaluation of employees to determine the retention level of information security policy and procedures. For example, using social engineering-based penetration testing techniques to determine how effectively employees follow policy, including attempts to get employees to share userid and password information.

Summary

Information Security is as much as a people issue as it is a technology issue. A benign act by an un-aware, un-educated government worker can create a significant vulnerability. Failure to provide effective Information Security awareness training to all government workers puts an agency's mission a great risk and jeopardizes the safety and security of our entire nation. However, with the appropriate focus on information security awareness, our nation's information assets will be better protected by the government workers who use them on a daily basis.

Contact Information

SecureInfo Corporation is a market-proven provider of Information Assurance solutions, enabling Federal organizations to understand, document and mitigate information security risk; assure information systems are secure; reduce security costs and achieve and demonstrate compliance with NIST, DIACAP and FISMA requirements.

Media Contact

Chris Leach
Welz & Weisel Communications
703.218.3555
chris@w2comm.com

SecureInfo Corporation

1410 Spring Hill Road
McLean, VA 22102
Office: (703) 245-9700
www.secureinfo.com

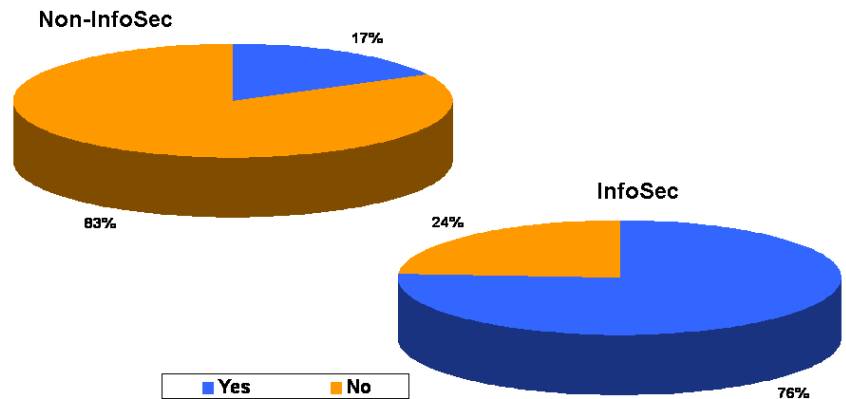
Appendix

Agency Security Awareness Training Results²

Agency	CIO Report – # of Employees that Received Security Awareness Training	CIO Report – % of Workers that Received Awareness Training	IG Report - “The agency has ensured security training and awareness of all employees”	Total Cost for Providing IT Security Training
US Agency for International Development	8,417	100%	Almost Always (96-100% of employees)	\$30,000
Department of Agriculture	110,019	99%	Almost Always (96-100% of employees)	\$435,542
Department of Commerce	44,049	98%	Mostly (81-95% of employees)	\$1,110,500
Department of Defense	2,068,594	88%	Sometimes (51-70% of employees)	\$38,084,955
Department of Education	10,342	99%	Almost Always (96-100% of employees)	\$411,178
Department of Energy	136,111	97%	Almost Always (96-100% of employees)	\$10,552,764
Environmental Protection Agency	20,618	100%	Almost Always (96-100% of employees)	\$614,000
General Services Administration	15,111	100%	Almost Always (96-100% of employees)	\$150,000
Department of Health and Human Services	85,690	99%	Frequently (71-80% of employees)	\$2,423,731
Department of Homeland Security	155,212	75%	Frequently (71-80% of employees)	\$2,276,002
Department of Housing and Urban Development	8,236	97%	Almost Always (96-100% of employees)	\$60,000
Department of the Interior	72,621	98%	Mostly (81-95% of employees)	\$998,272
Department of Justice	117,688	96%	Almost Always (96-100% of employees)	\$3,053,048
Department of Labor	16,972	96%	Almost Always (96-100% of employees)	\$149,038
National Aeronautics and Space Administration	56,109	92%	Almost Always (96-100% of employees)	\$1,200,000
National Science Foundation	4,431	97%	Mostly (81-95% of employees)	\$77,500
Nuclear Regulatory Commission	3,670	99%	Mostly (81-95% of employees)	\$315,000
Office of Personnel Management	5,165	100%	Almost Always (96-100% of employees)	\$101,712
Small Business Administration	4,851	74%	Mostly (81-95% of employees)	\$20,300
Smithsonian Institution	7,089	95%	Frequently (71-80% of employees)	\$4,658
Social Security Administration	65,236	100%	Mostly (81-95% of employees)	\$368,810
Department of State	52,913	100%	Frequently (71-80% of employees)	\$2,976,000
Department of Transportation	66,706	91%	Mostly (81-95% of employees)	\$1,577,443
Department of the Treasury	121,224	98%	Mostly (81-95% of employees)	\$2,280,126
Department of Veterans Affairs	234,216	99%	Rarely (0-50% of employees)	\$4,862,000
Totals	3,491,290	95% (Average)	Almost Always – 11 Agencies Frequently – 4 Agencies Mostly – 8 Agencies Sometimes – 1 Agency Rarely – 1 Agency	\$74,132,579

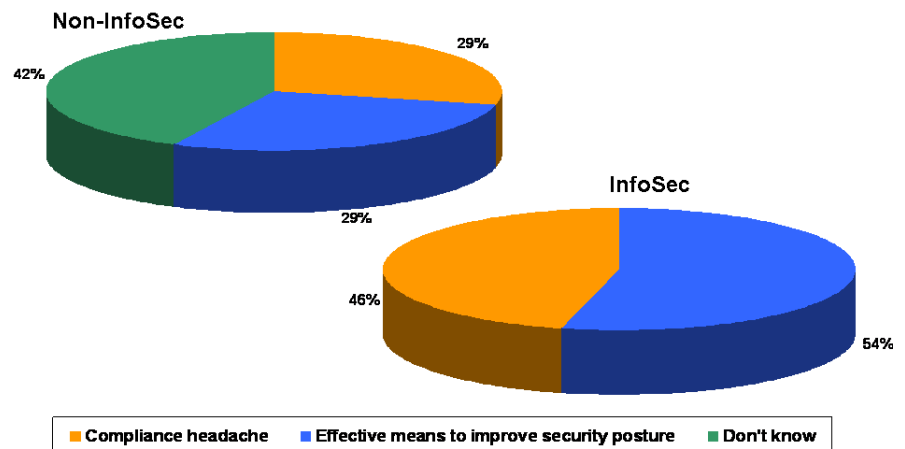
**Supplemental Results –
Information Security vs. Non-Information Security Professionals**

Eighty three percent of non-information security professionals have not heard of FISMA while 24% of information security professionals have not heard of FISMA.



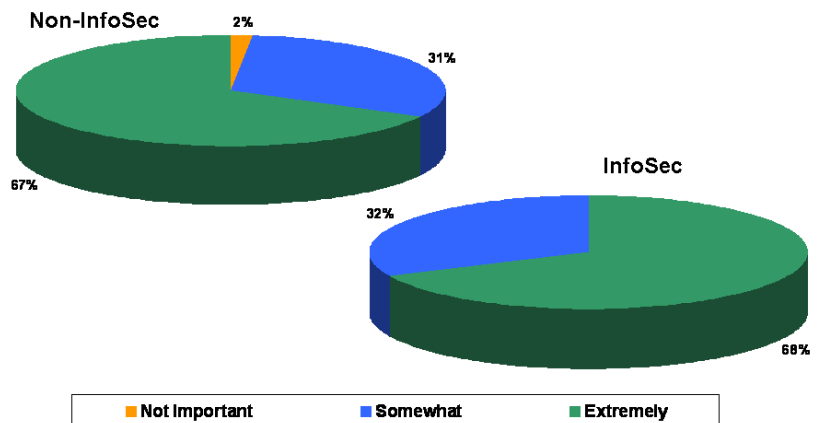
Have you heard of FISMA?

Thirty percent of non-information security professionals who have heard of FISMA believe their agency views FISMA as a compliance headache while nearly half (46%) of information security professionals surveyed believe their agency views FISMA as a compliance headache.



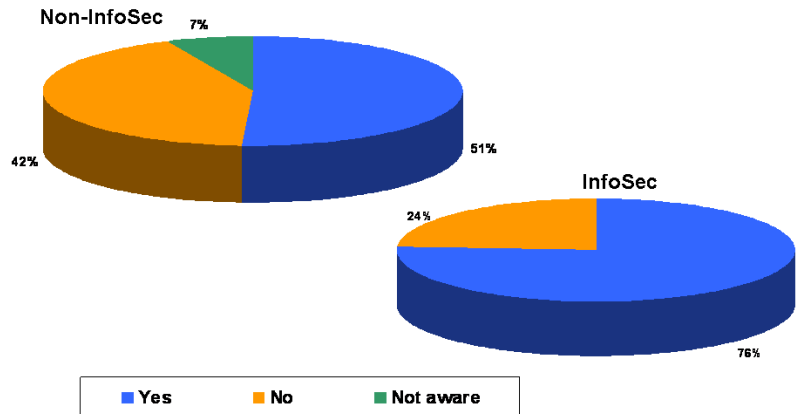
How does your organization view FISMA?

Two thirds (67% and 68% respectively) of non-information security professionals and information security professionals believe information security is extremely important for achieving agency goals



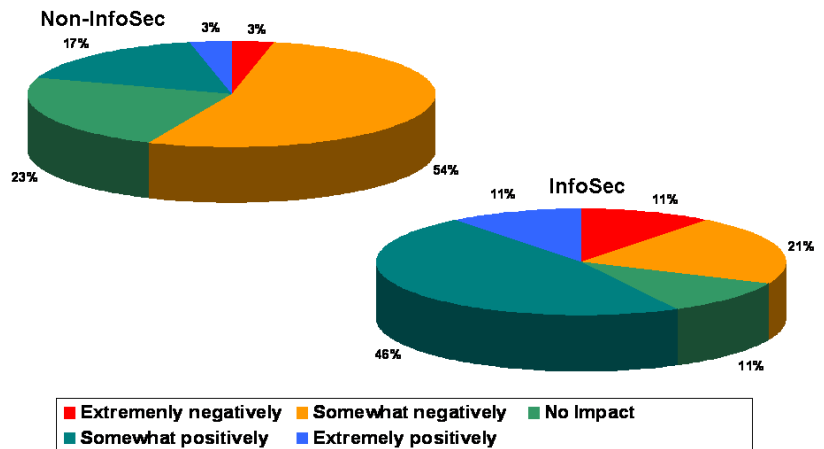
How important is information security for achieving your organization's overall business goals?

Half of non-information security professionals (51%) believe their job has been affected by changes in information security policy while three quarters (75%) of information security professionals believe their job has been affected.



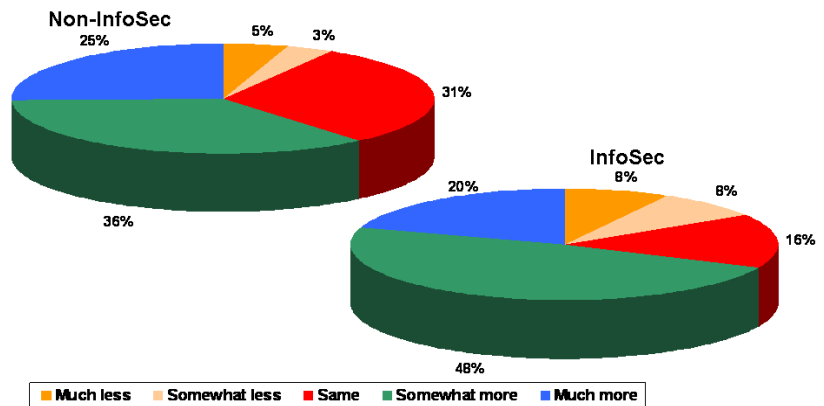
Has your job been affected over the past 12 months due to changes in information security policies and or/controls?

More than half (57%) of non information security professionals believe their job has been negatively impacted by changes in information security policies while one third (32%) of information security professionals believe their job has been negatively impacted.



Has your productivity/effectiveness been impacted by changes in security policy/or controls?

Sixty one percent of non-information security professionals believe their respective agencies are more secure than last year. Sixty eight percent of information security professionals believe their respective agencies are more secure than last year.



Do you think your agency is more secure today than a year ago?

Footnotes

1. NIST Special Publication 800-50, Building an Information Technology Security Awareness and Training Program, October 2003
2. The FISMA Report to Congress on the Implementation of FISMA, March 1, 2007