GOVERNMENT SECURITY PRACTITIONER SURVEY:
COUNTDOWN TO CONTINUOUS MONITORING

Dimensional Research | December 2011

Introduction

In today's IT environment, U.S. federal organizations face a wide range of electronic adversaries, including hackers that develop ever more complex and diverse attacks designed for the specific purpose of stealing government data – typically sold to the highest bidders – and even foreign nation states that aggressively pursue both development of such nefarious campaigns, and acquisition of the information they harvest.

In response, and to advance federal agencies beyond traditional risk assessment models considered less proactive, White House regulators have ordered all organizations to implement continuous monitoring, a more frequent, repeatable, method of measuring risk.

To ensure compliance with the mandate, first included in the Federal Information Security Management Act (FISMA) in late 2010, White House officials set a requirement for agencies to have continuous monitoring broadly deployed by the end of fiscal 2012 (Sept 30).

Specifications for these systems are outlined in the National Institute of Standards and Technology (NIST) SP 800-137: Guide for Continuous Monitoring of Information Systems and Organizations, with the deadline issued and to be enforced by the White House Office of Management and Budget (OMB).

However, many questions remain as to how well agencies will fare in meeting the OMB's expectations; Are agencies progressing to meet the regulations and requirements? Will data ultimately be made more secure? What tools are considered most effective and required to meet these federal requirements?

RedSeal Networks commissioned Dimensional Research to investigate and report the answers to these important questions.

This report reveals responses from over 200 security experts surveyed while attending the 2011 7th Annual GFIRST National Conference. Representatives sharing the name of their employer represented nearly every major U.S. federal agency including every arm of the military, most cabinets and many of the largest U.S. government contractors.

Executive Summary

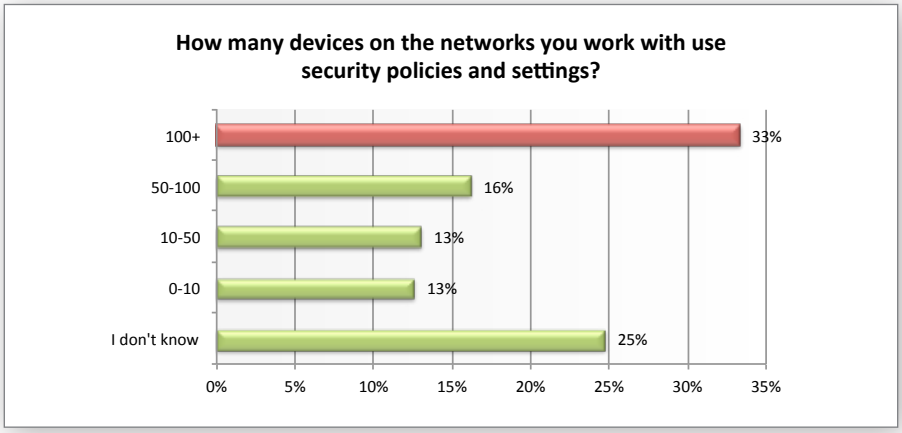
- **A majority of agencies will fail to comply with 2012 federal security requirements**
  - Only 28% of agency executives stated they will have the tools and processes in place to meet 2012 security mandates
  - 55% of the agencies revealed they won't be ready or don't know if they'll meet the September 2012 FISMA requirement
  - 33% of small agencies indicated they will have required security measures in place to meet requirements
- **Security solution implementation will be challenging**
  - Only 22% of federal agencies have already deployed mandated continuous monitoring solutions as ordered
  - 33% of the federal agencies indicated they have over 100 devices that require security configurations

- **Federal security experts agree that 2012 mandates will improve overall security**
  - 64% indicated that continuous monitoring and security metrics will improve overall security
  - 43% stated that network security device configuration and audit tools will improve security effectiveness and meet federal mandates

Detailed Findings

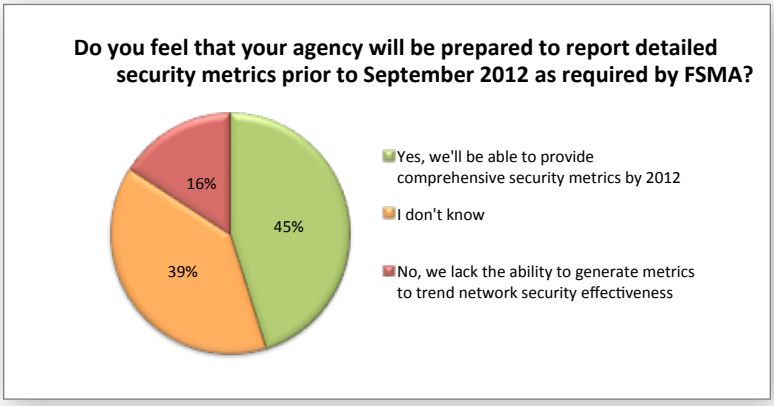
Large numbers of devices indicate complex and challenging security tasks

33% of government networks have over 100 devices that require security configurations. The largest agencies indicated they utilize thousands of devices that affect their security defenses. Each device must be properly configured to implement security policy and strategies and which now must also support continuous monitoring. 25% represented that they didn't even know how many devices contained security policy enforcement, revealing an unknown security risk.



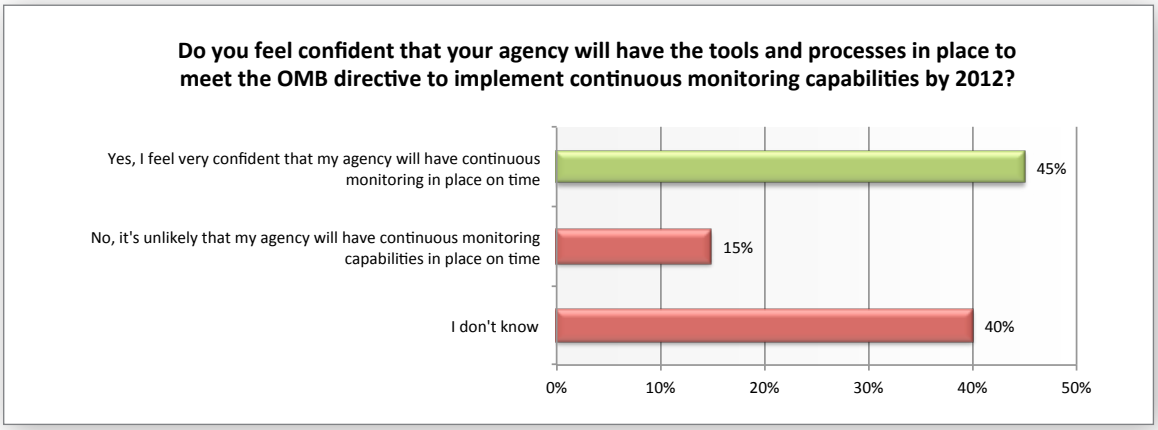
A majority admit that their agency will not be prepared to meet FISMA September 2012 deadline

Despite the impending requirement, 55% of the respondents reported they will not be able to meet the September 2012 deadline or lack the knowledge of compliance preparation status. While 45% do feel they are prepared, still more than half of all agencies indicated they will likely fail to meet requirements for mandated security reporting.



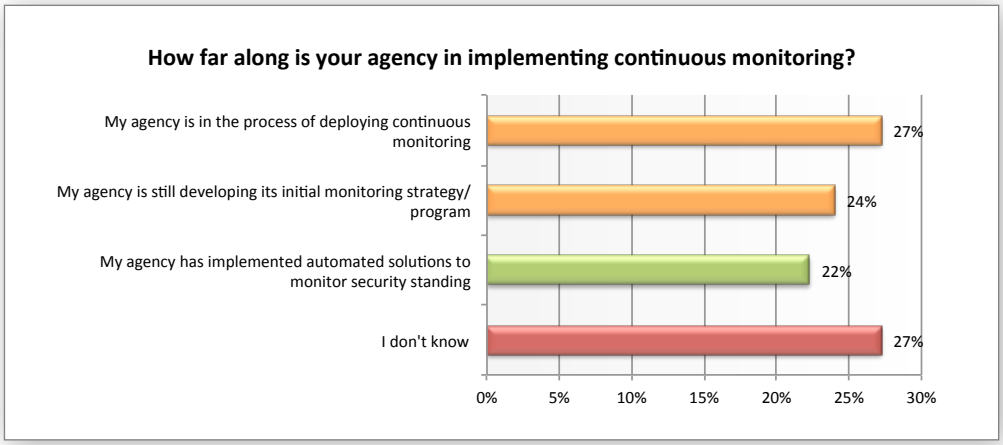
Most agencies lack the tools and processes to meet the impending 2012 OMB directives

The majority of the agencies at 55% stated they do not have the tools necessary to meet the OMB directive or are unaware if they do, making compliance unlikely. With only months until the directive is in effect, only 45% feel prepared and confident about meeting the requirements



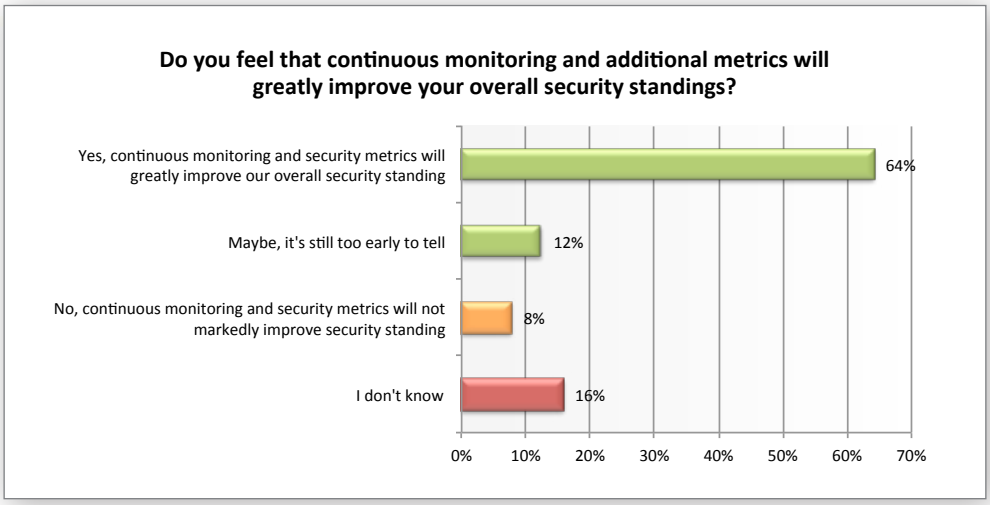
Most organizations are still planning and deploying their monitoring solutions required by 2012

At 51%, more than half of all agencies are still strategizing and implementing the monitoring mandated to be in effect in 2012. Only 22% of agencies reported being ready for the 2012 OMD and FISMA requirements, and 27% revealed they don't know their compliance progress or status.



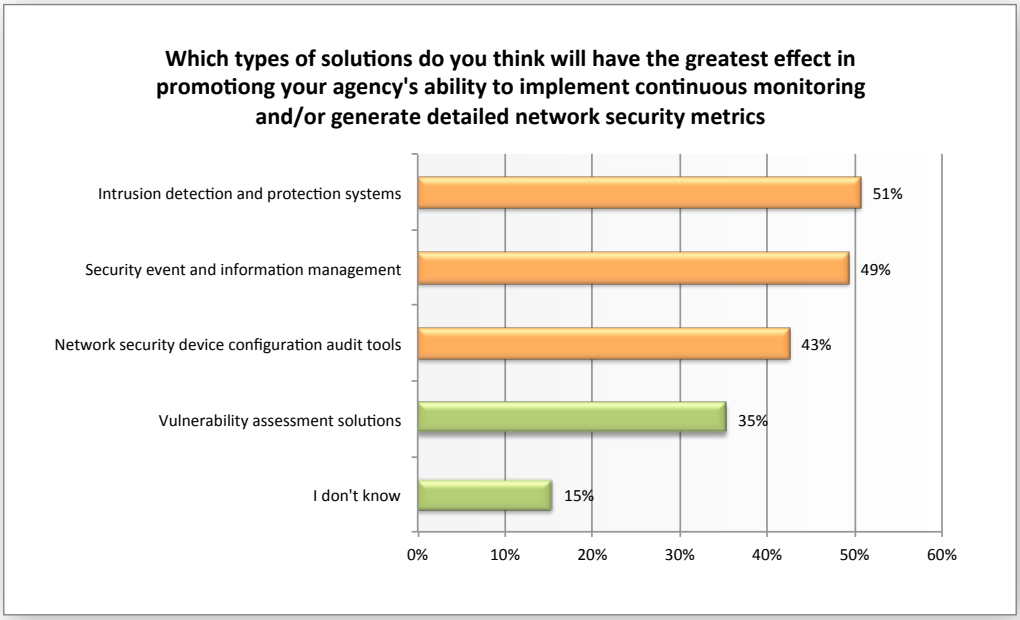
Most respondents believe that security monitoring will improve overall security

An overwhelming majority of respondents at 64% indicated that the continuous monitoring with increased measurement and use of security metrics will improve overall security management. Only 8% said that the added information will not aid or improve their organization's security standing.



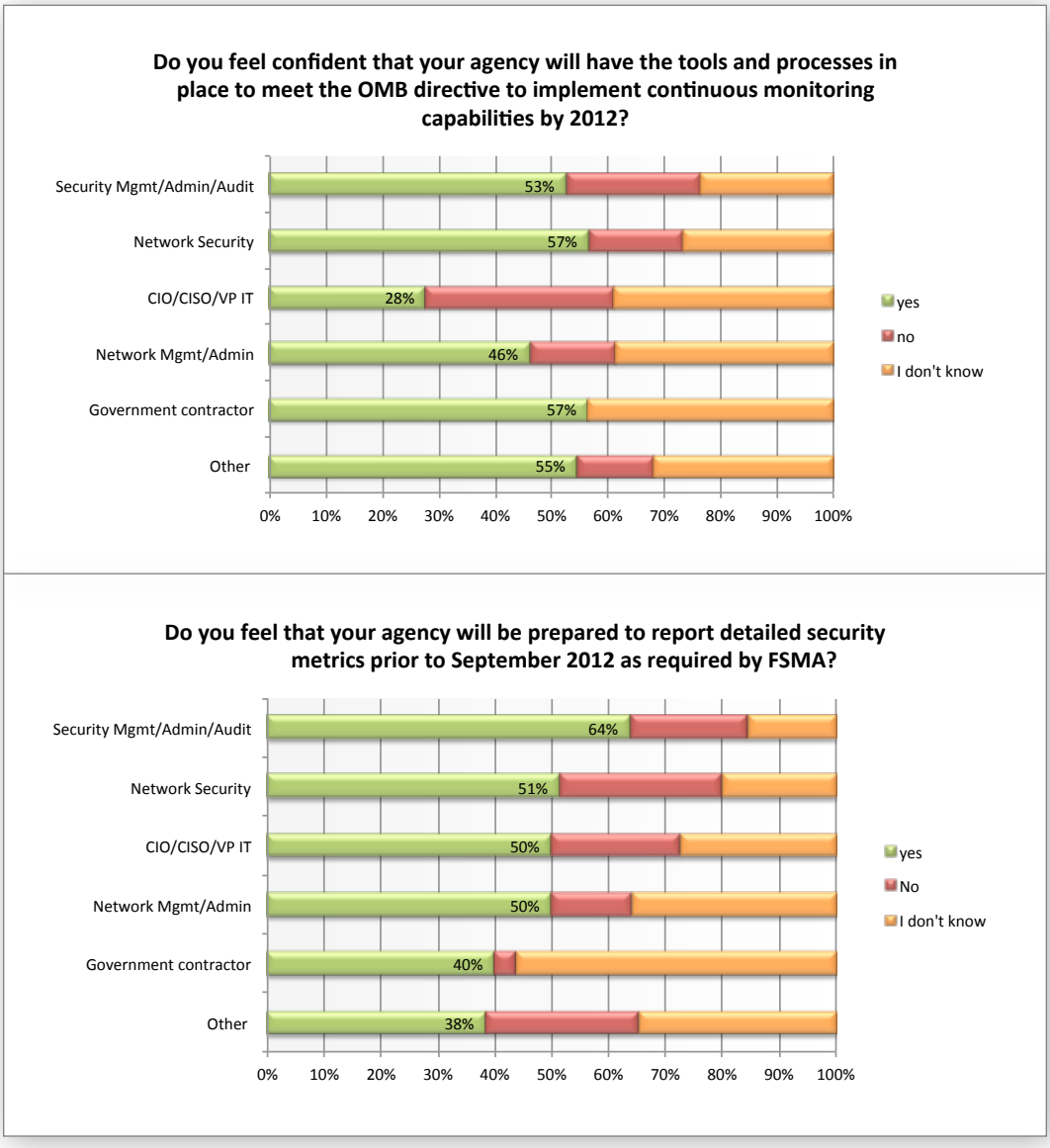
Combination of security tools and solutions needed to meet security requirements

Only 8% separates the top three security solutions selected by respondents which provide the technology needed to meet continuous monitoring objectives. This data indicates that a combination of security solutions will increase an agency's ability to achieve federally mandated requirements.



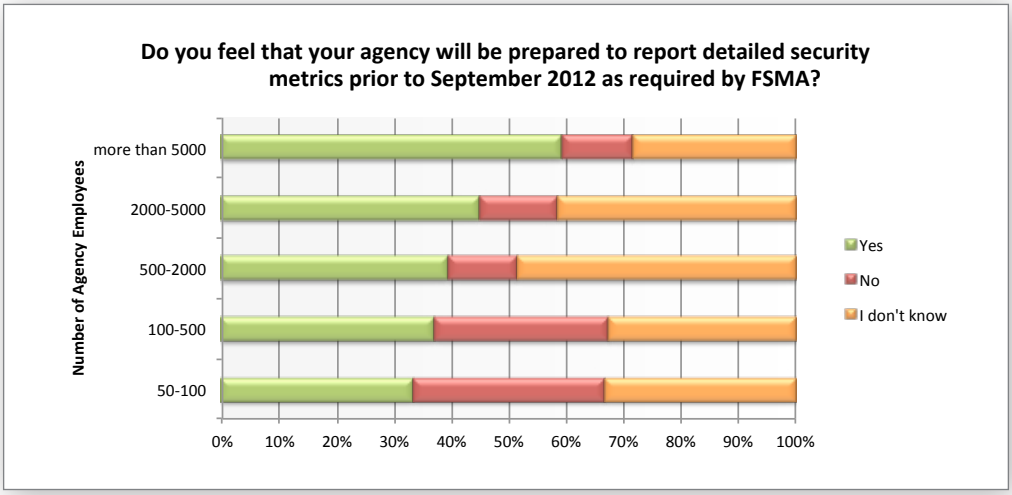
Most agency executives indicated they will fail to meet the 2012 security requirements

In a revealing response, only 28% of executives believe they will have the proper tools and process in place to meet the 2012 federally mandated security monitoring requirements. Only 50% of all executives said they will be prepared to provide the security metrics required by FISMA in that same timeframe.



Larger agencies reported being better prepared for achieving 2012 security mandates

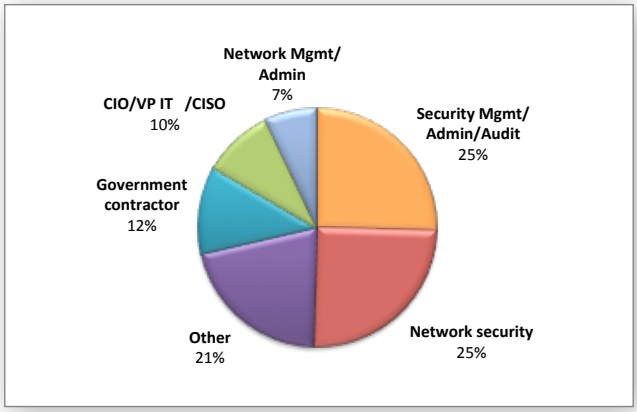
59% of the largest agencies, with more than 5000 employees, indicated they expect to meet federal mandates. However the smaller the agency, the less likely they will meet the same requirements. Only 33% of the smallest agencies stated they will achieve the requirements, nearly half the number of the largest agencies surveyed.



Demographics

Broad spectrum of roles directly involved with security polices and implementation

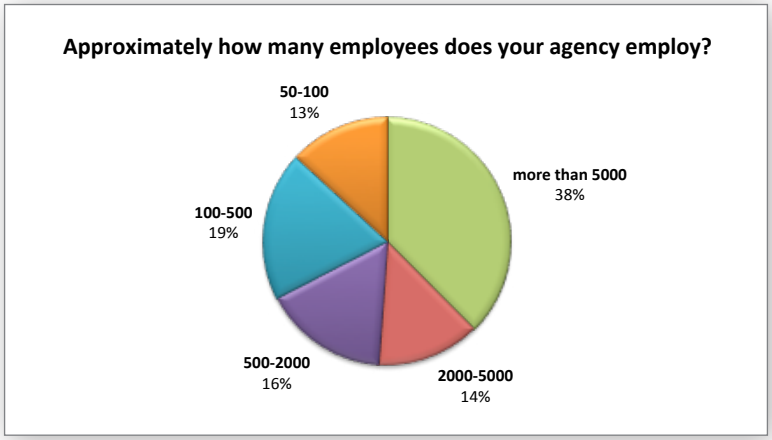
Survey participants reported the following titles when describing their role in the company: Security Management, Security Administration, Security Audit, Network Security, Network Management and Network Administration, government contractor, Chief Information Security Officer (CISO), Chief Information Officer (CIO) and Vice President IT. Respondents were directly employed by government agencies either as government employees or as contractors or consultants.



*Other titles included forensics, military specialist, security architect, security assessment, security developer, security consultant, operations, and VP special task force but individually, none represented more than 2%.

Large and small agencies well represented

Survey participants provided valuable visibility into both ends of the spectrum with 52% from agencies employing over 2000 individuals and 32% from small agencies with fewer than 500 employees.



Agencies represented were CSC, VA, DHS, DIS, ELET, EPA, FAA, FCC, FLEFC, FTC, IRS, JMU, KGG, NASA, SSA, Treasury, TSA, TVA, US Army, USAF, USCG, USMC, US Navy, USPS and several state and county agencies.

Survey Methodology

The survey was administered to attendees at the 2011 7th Annual GFIRST National Conference. It was conducted on the tradeshow floor in the RedSeal booth. The research was commissioned to gather data on agencies' ability to meet the 2012 federal security and monitoring mandates as outlined in the OMB and FISMA directives.

This report was prepared in December 2011 based on responses from 234 security professionals. The survey sponsor, RedSeal, was revealed to participants prior to their participation. Although drawings for an iPad were offered, survey participation was not required for eligibility.

About Dimensional Research

Dimensional Research® provides practical marketing research to help technology companies make their customers more successful. Our researchers are experts in the people, processes, and technology of corporate IT and understand how corporate IT organizations operate. We partner with our clients to deliver actionable information that reduces risks, increases customer satisfaction, and grows the business. For more information visit www.dimensionalresearch.com.

About RedSeal

RedSeal Networks enables our customers' IT security management and staff to continuously understand the security state and regulatory compliance of their network and information systems, recognize the resulting risk to their operations and assets, and identify and drive actions to improve security and reduce risk. Unlike systems that measure the impact of attacks after they occur, RedSeal analyzes the complex interaction of all network security controls, delivering in-depth understanding of security performance, continuous compliance, and actionable steps for risk remediation. For more information on RedSeal products please visit the company's web site at www.redsealnetworks.com and follow us on Twitter @RedSealNetworks.