Analyze the Future

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com

WHITE PAPER

2006 Global Information Security Workforce Study: A Special U.S. Government Perspective

Sponsored by: (ISC)^2

Allan Carey

December 2006

IDC OPINION

Information and systems security is paramount in government and private sector environments and is driven largely by asset protection, privacy, and business continuity responsibilities. Governments are held to a very high standard in maintaining public trust and policymaker confidence to protect citizen privacy and provide for the continuity of government. This responsibility has become even more critical in light of recent information breaches, terrorism events, and natural disasters. Private sector organizations must maintain consumer confidence and, in many regulated industries, protect consumers from physical and economic harm. Both public and private sector organizations recognize their heightened accountability and are reacting to security requirements — driven by either regulatory compliance or long-term survivability — with significant financial commitments in qualified personnel to manage their information security programs.

This study is an adaptation of the 2006 *Global Information Security Workforce Study* (*GISWS)*. It is designed to reflect the opinions of the government information security workforce currently employed in the United States at the federal, state, and local levels and provide a glimpse into the future of the information security profession. IDC believes the following factors will keep information security high on the U.S. government's priority list for the foreseeable future:

- Increasing regulatory pressure within the public sector will keep the focus on strong security policies, processes, and controls, which will force organizations to adopt security standards and frameworks for a long-term approach to mitigating risk.
- Digital threats, attacks, and cyber warfare are becoming more targeted and sophisticated, which will require security professionals to learn new skills and techniques to abate the threats and minimize damage.
- Both physical and logical securities are continuously at risk, which means that security is now everyone's responsibility within government organizations.
- Custodianship of large volumes of consumer data places significant responsibility and accountability on government organizations to uphold citizens' rights to privacy and confidentiality.

EXECUTIVE SUMMARY

The International Information Systems Security Certification Consortium, (ISC)^2, engaged IDC for the third consecutive year to provide detailed insight into the important trends and opportunities emerging in the information security profession worldwide. The electronic survey was conducted via a Web-based portal, where out of 4,016 total responses, 373 respondents from the U.S. public sector, both agency employees and contractors, offered their opinions about the information security profession in which they are employed. Topics covered in the survey range from the amount of information security education and training received to the value of certifications to new areas where additional training is required.

Some key findings of this year's study pertaining to the U.S. government are the following:

- Public sector compliance requirements are fueling the demand for information security solutions and qualified staff.
- The top three activities that consume the most amount of time of information security professionals in the U.S. federal government are achieving certification and accreditation (C&A) of information systems, meeting regulatory compliance, and researching new technologies.
- Common security technology areas being implemented in the next 12 months by government organizations across the United States are biometrics, wireless security, and forensics tools.
- U.S. government organizations are spending an average of more than 46% of their security budgets on personnel and training.
- U.S. federal Department of Defense (DoD) respondents average 10.5 years of information security experience and $98,052 in salary.
- U.S. federal non-DoD respondents average 11.2 years of information security experience and $107,957 in salary.
- U.S. state and local (S&L) respondents average 10.2 years of information security experience and $79,709 in salary.
- Security professionals are asking for additional education and training in the areas of information risk management, forensics, and C&A.

U.S. government officials from the executive branch down through the chain of command to the S&L level recognize that information security is a global, governmentwide priority that cannot be addressed through the sole use of technology solutions. The commitment of the U.S. government is required at the financial, management, and operational levels to proactively secure and protect the nation's logical and physical assets. Effective security management requires the dynamic balance between people, policies, processes, and technology to effectively mitigate the risks associated with being digitally connected and participating in an information-sharing, intelligence-driven environment.

METHODOLOGY

The 2006 *Global Information Security Workforce Study (GISWS)* was conducted during the summer of 2006 on behalf of (ISC)^2, a nonprofit organization dedicated to providing education, certification, and peer-networking opportunities for information security professionals worldwide. (ISC)^2 engaged IDC for the third consecutive year to provide detailed insight into the important trends and opportunities in the profession worldwide. The objective of this workforce study is to provide meaningful research data about the information security profession to industry stakeholders, such as professionals, corporations, government agencies, (ISC)^2 members, academia, and other interested parties such as hiring managers. The electronic survey portion of this study was conducted via a Web-based portal, with traffic driven to the site through the use of email solicitations. IDC surveyed 4,016 respondents from companies and public sector organizations around the globe to gather their opinions about the information security profession. The Web-based surveys were targeted to query information security profession respondents worldwide. Additionally, IDC supplemented the analysis with its other primary data sources and methods. Several questions were asked to determine the eligibility of respondents. Respondents were screened for the following:

- Responsibility for acquiring or managing their organizations' information security
- Involvement in the decision-making process regarding the use of security technology and services and/or the hiring of internal security staff
- Employment in the information security profession

While reading through this study, keep in mind that the sample population is not designed to reflect the universe of all public sector organizations; therefore, the results should not be projected across the entire population. The data points are meant to be interpreted as leading market indicators and reflect the opinions of the 373 government respondents in the United States who took part in the 2006 *GISWS*.

Note: All monetary figures stated throughout this study are in U.S. dollars.

SITUATION OVERVIEW

Introduction

Recent high-profile security breaches in government agencies have highlighted a need for more effective governance structure and monitoring of information security policy. These breaches reveal that information security gaps occur more frequently in the areas of policy, process, and people errors than through technology failures. For example, the case of a stolen Department of Veterans Affairs laptop containing over 26 million records of personal information led to a hearing by the House Committee on Government Reform in June 2006 that examined the operational aspects of information technology as it applies to organizational management and data security at federal agencies. During that hearing, the committee chairperson called for federal agencies to report all data breaches since 2003 to the committee. Nineteen agencies reported a total of 1,788 losses, likely a conservative number at best. It was also determined that it is not uncommon for agencies to be unaware of data breaches; typically, a situation is made apparent via an assessment, audit or exposure. Other instances from 2006 involved the U.S. Department of Agriculture exposing Social Security numbers, malicious hackers accessing a Tricare Management Activity public server at DoD, and Chinese hackers attacking the Web systems at the U.S. Department of Commerce.

In government, the rise in cyber terrorism has led to security policies and mandates, such as the Federal Information Security Management Act (FISMA), the Health Insurance Portability and Accountability Act (HIPAA), and Homeland Security Presidential Directive-12 (HSPD-12), that are designed to protect the public interest and compel mandatory behavior by government agencies. Private sector organizations are vulnerable primarily to economic damage from inadequate security, but they too are increasingly coming under regulatory schemes to assure consumer protection. Whether driven by government mandate or economic incentive, both public and private sector organizations recognize and are responding to security imperatives with substantial investments in trained personnel to manage them.

Accordingly, the growing demand for qualified information security professionals among U.S. government entities will remain a priority for the foreseeable future as organizations seek individuals with both technical and business skills, such as collaboration, communication, and negotiation. Government agencies will be competing with the private sector for experienced and certified information security professionals who can provide leadership and best practices in the areas of policy, processes, and management.

Study Demographics

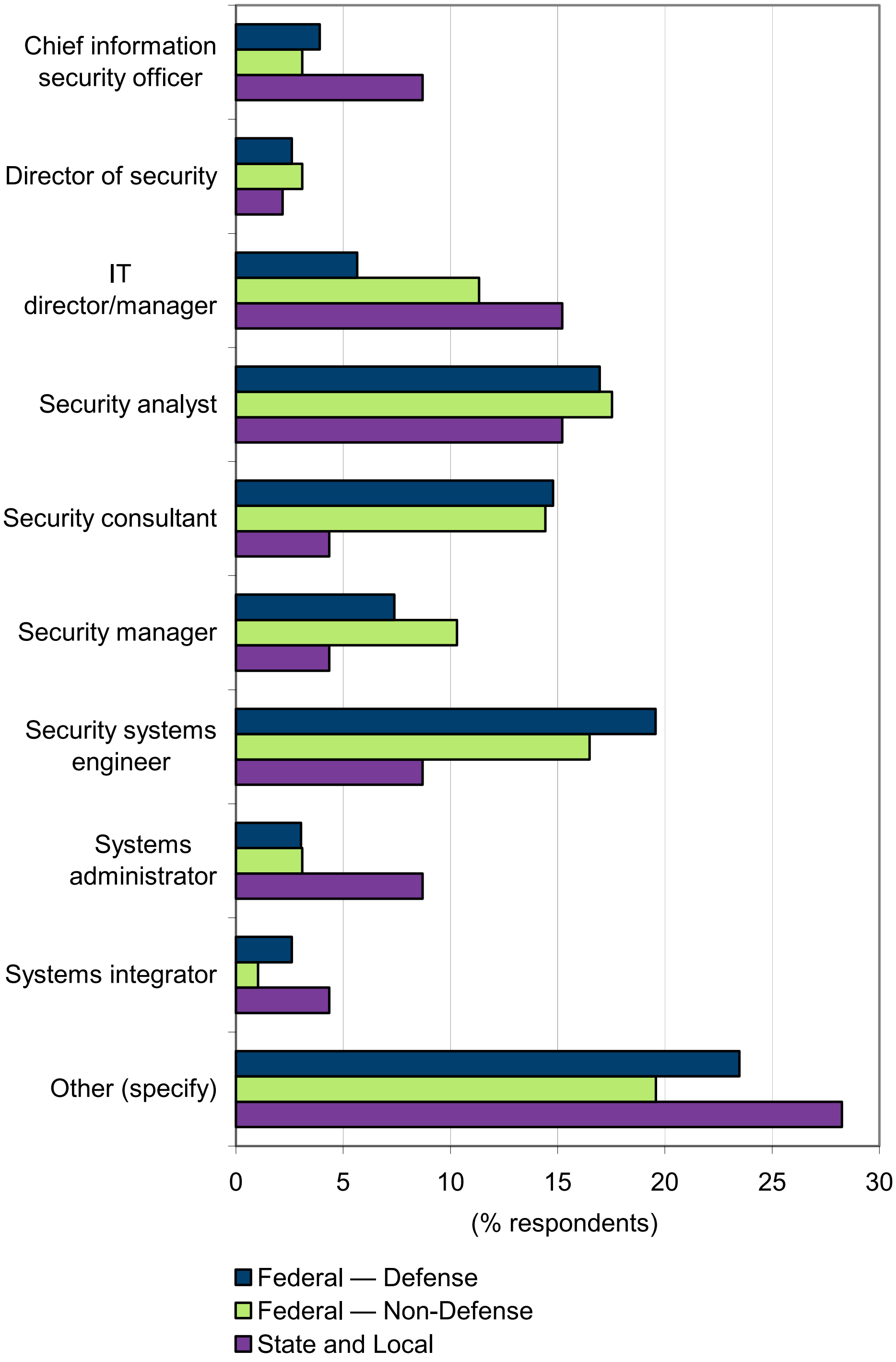
This year's study reached 373 government information security professionals across the United States. Respondents came from three major areas of government: federal (defense) (62%), federal (non-defense) (26%), and S&L (12%). The majority of respondents are government employees, but a percentage of respondents within each area work on a contractor basis: federal (defense) (20%), federal (non-defense) (24%), and S&L (7%).

Each respondent is involved, in some capacity, in information security decisions, ranging from technology selection to security management to hiring staff. Their job functions and titles range from security analyst to chief information security officer (CISO). Figure 1 illustrates the variation in titles from federal to S&L information security professionals. The most common federal positions include security analyst and security systems engineer, while security analyst and IT director or manager are common at the S&L level. Individuals with sole responsibility for physical security are not included in this study.

Information security professionals surveyed this year represent organizations of all sizes. Large organizations (10,000+ employees) account for more than 60% of respondents at the federal level. Approximately 4 out of 10 are employed by S&L organizations with more than 1,000 but less than 10,000 employees. Very few organizations have less than 10 employees (see Figure 2).

FIGURE 1

Respondent by Job Title or Function



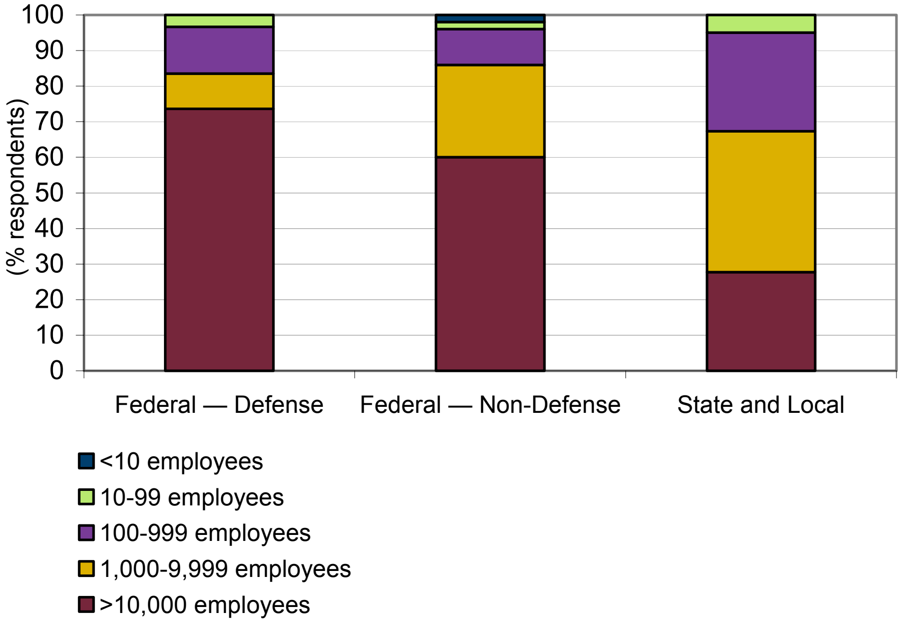
n = 373

Note: Other represents titles such as chief security officer, IT auditor and security architect.

Source: IDC's *Global Information Security Workforce Study*, 2006

FIGURE 2

Respondents by Organization Size



n = 365

Source: IDC's *Global Information Security Workforce Study*, 2006

Initiatives and Objectives Within the Next 12 Months

Achieving C&A of information systems, meeting regulatory compliance, and researching new technologies consume a significant amount of time for information security professionals in the U.S. federal government. Their colleagues employed by U.S. state and local governments have slightly different priorities on a daily basis: researching new technologies, dealing with internal politics, meeting compliance, and monitoring their networks for malicious activity. Table 1 emphasizes the top five security areas/solutions each government segment plans to deploy over the next 12 months with the hope that these initiatives will alleviate some of their operational challenges and free more time to focus on strategic initiatives. Some common security technology areas being implemented by organizations across governments are biometrics, wireless security, and forensics tools.

Biometrics was mentioned as the number one security technology implementation across U.S. government agencies and organizations. Biometrics such as fingerprints and facial recognition are being leveraged as an additional credential that is linked to an individual's identity for verification purposes (e.g., common access cards as a result of HSPD-12). Biometrics could find extended use throughout the federal government because most federal agencies seem to have met the October 2006 deadline for implementing the capability to issue HSPD-12 compliant credentials and GSA's forthcoming contracts will extend the capability across the full breadth of the federal government .

Another area of common interest is wireless security solutions. As more data traverses the airwaves, it is critical that information be exchanged in a secure and protected environment. In a time of crisis or national security, individuals receiving intelligence or instructions need assurance that the data is reliable and originated from a trusted source. Wireless security will become even more important as voice over IP (VoIP) is adopted and both voice and data flow over the same wireless IP-based networks.

In addition, forensics has become a key part of any information security program. Effectively dealing with, mitigating, responding to, and prosecuting computer-related abuse and crimes clearly are among the greatest challenges for information security professionals and auditors. There is a burgeoning need for decisive answers, quick responses, and evidence preservation to document attacks and system compromises that may cripple or completely disable any government computer system. The interest in and demand for security investigation and e-discovery capabilities are the result of a number of investigations stemming from insider threats and breaches to government information systems.

TABLE 1

Top 5 Security Technologies Being Deployed by Segment

Rank	Federal — Defense	Federal — Non-Defense	State and Local
1	Biometrics	Biometrics	Biometrics
2	Wireless security solutions	Wireless security solutions	Identity and access management
3	Intrusion prevention	Intrusion prevention	Wireless security solutions
4	Forensics	Forensics	Security event or information management
5	Compliance management	Cryptography	Compliance management

Source: IDC's *Global Information Security Workforce Study*, 2006

On average, government organizations across the United States are spending 46% of their security budgets on personnel and training to support their information security strategies and programs, compared to an average of 43% in 2005. By comparison, U.S. private sector enterprises are allocating a slightly higher percentage (49%) of their information security budgets on personnel and training this year. This number includes all expenses to attract, hire, and retain qualified security professionals required to execute an organization's security strategy and achieve its business objectives. In addition, any internal and external security-related training delivered to employees is captured.

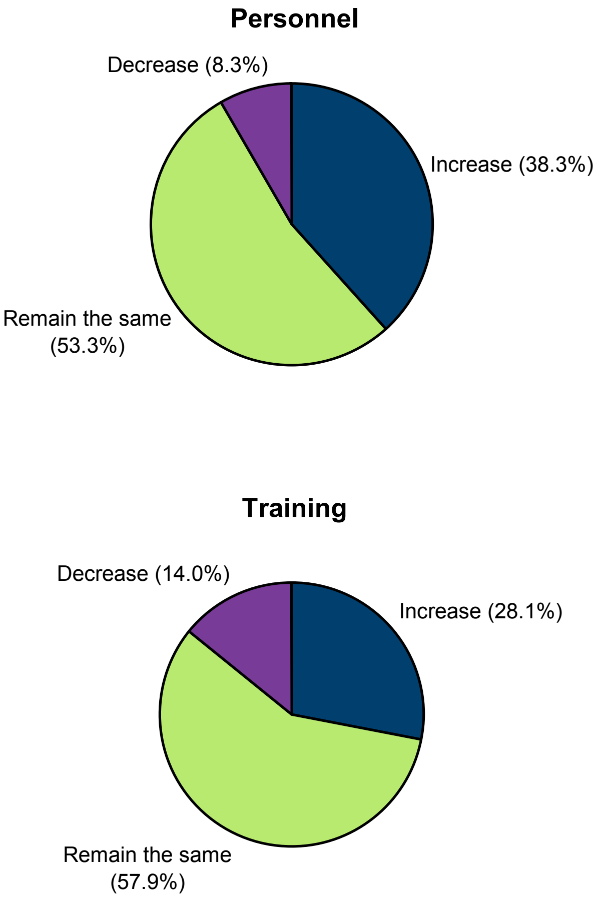
Over the next 12 months, approximately 53% of U.S. government information security professionals believe staffing as a percentage of the information security budget will remain the same (see Figure 3). Another 38% of respondents indicated they expect an increase in spending on personnel. From the U.S. private sector perspective, 46% of respondents expect to see an increase in personnel expenditures, while 48% think it will remain the same. Therefore, information security professionals in the U.S. private sector are slightly more optimistic than their counterparts in government about the prospect of potentially getting more staff resources and/or wage increases.

On a related topic, almost 6 out of 10 government security professionals believe spending on training and education will remain the same in 2007 as it was for 2006. The 28% of individuals across the government segments expecting to see an increase in training spending predict an average 26% increase for 2007. A similar expected increase in 2007 was expressed by 32% of respondents in the U.S. private sector.

Requiring qualified and experienced personnel to possess a variety of skill sets such as forensics, business continuity and disaster recovery planning, and C&A will be critical to the success of government agencies as they employ new and emerging technologies, and build out risk management programs. Continuous training and education will be instrumental in enabling information security professionals and their employers to meet government mandates, including FISMA and DoD Directive 8570.1. As a point of reference, the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST) offer good guidance and a framework for protecting government data; however, that guidance lacks coordinated governmentwide implementation. In its report on the VA laptop theft, for example, the Government Accountability Office (GAO) recommended "strong leadership, sustained management commitment and effort, disciplined processes, and consistent oversight." This implies the need for management buy-in and accountability and the expertise of trained professionals to drive awareness and successful execution of agency-specific policies.

FIGURE 3

U.S. Government Expected Change in Amount of Information Security-Related Spending — Next 12 Months



Source: IDC's *Global Information Security Workforce Study*, 2006

Profile: The Public Sector Information Security Professional

Across the various U.S. government organizations represented in this study, respondents reported achieving a high level of education (see Figure 4). On average, the government information security workforce consists of 87% individuals with at least a bachelor's degree from a higher education institution. This is on par with private sector organizations. Interestingly, federal defense agencies employ a higher percentage of individuals with a master's degree than other segments of the government and more than private sector enterprises.

Another candidate criterion, years of professional experience, proved to be important to hiring managers and their organizations during the candidate evaluation and selection process (see Table 2). Survey results indicated that non-defense–related federal agencies tend to employ information security professionals with slightly higher average years of experience (11.2 years) than other segments of government (defense: 10.5 years and S&L: 10.2 years). In contrast, the average information security professional in the private sector has 9.9 years of experience. Information security professionals working in government agencies tend to have more years of information security experience than those in non-government positions. One possible explanation for this difference is the fact that government, directed by regulations such as National Security Decision Directive 145 and the Computer Security Act of 1987 and guided by the National Institute of Standards and Technology and the Office of Management and Budget, has been concerned with information security for a longer time than the private sector. This is especially true for the Department of Defense. In addition, the difference could be attributed to the relative career stability of government-sector jobs. Many workers enjoy the stability and benefits offered by public-sector employment and often stay with those jobs longer.

A pitfall to this experienced, aging workforce in government is that they are reaching retirement age. DoD departmental policies for hiring and retaining employees have not significantly changed over the past few years to compensate for the realities of the IT workforce. Most young employees are not looking for long-term employment opportunities and career security — they want new experiences and challenges. They also expect access to newer technologies to perform their jobs and be productive. U.S government agencies must adapt their policies and programs for attracting younger employees to backfill open positions left behind by the soon-to-be-retiring skilled workforce.

Consequently, Figure 5 displays the salary differences between U.S. federal (defense and non-defense) and S&L government respondents and how the differences compare with responses from information security professionals in other U.S. industries. The federal non-defense respondents reported the highest average salary of $107,957, which interestingly correlates to their average of 11.2 years of information security experience. Last year, employees within non-defense agencies stated an average salary of $98,000 with an average of 10.6 years of experience. On the defense side, federal respondents generated an average salary of $98,052 (up from $96,000 in 2005), which represents a 23% increase over the average salary of an information security professional employed by a state or local government. Private sector respondents displayed an average salary of $99,634. One advantage of private sector employers is their ability to offer generous compensation packages beyond salary and standard benefits to attract talented, qualified information security professionals, many of whom come from U.S. government backgrounds.

According to respondents this year, the ranking of reporting structures in defense remained relatively the same as reported in 2005. An increased amount (44%) of information security professionals directly report to the security or information assurance group, compared to 35% reporting to the same group in 2005. In both years, the second-ranked top area of reporting belonged to the CIO or equivalent executive, then followed by operations and IT in 2006 and 2005, respectively. Within non-defense, the lion's share (36%) of information security respondents reported to the security or information assurance group. This contrasts with responses from 2005, in which 39% of surveyed professionals indicated that they mainly reported to their IT departments. In 2006, the IT department has fallen to the third most-mentioned department, which would indicate that security has become a higher profile issue in non-defense agencies and, consequently, agencies shifted the reporting responsibility away from IT to the security and executive management levels.

Federal – Defense

Of the respondents employed by the U.S. federal government in the defense sector, 83% are men and 17% are women. Many respondents have either a master's (40%) or bachelor's (44%) degree. In aggregate, they have an average of 10.5 years of information security experience and receive $98,052 in salary.

Since the federal government places such a high degree of importance and emphasis on information assurance, it's no surprise that the security/information assurance group would carry a higher profile and be the top mentioned reporting group for information security professionals than in other government organizations. More than four out of every 10 defense respondents directly report into the security/information assurance group, slightly more than non-defense (36%) and significantly more than S&L respondents (11%). By comparison, 21% of respondents in other U.S. industries report to the security/information assurance group. The CIO or equivalent executive has 17% of all information security respondents under management, 1% less than information security professionals in other U.S. industries outside government. The third- and fourth-ranked reporting areas following the CIO were operations and the IT department.

Federal – Non-Defense

Of the respondents employed by the U.S. federal government in the non-defense sector, 79% are men and 21% are women. The majority of respondents have a bachelor's degree (53%), another 36% received a master's, and 1% achieved a doctorate. In aggregate, they have an average of 11.2 years of information security experience and receive $107,957 in salary.

The security/information assurance group within federal non-defense agencies has 36% of information security professionals reporting into it, similar to their peers in the defense sector. The CIO or equivalent executive has 27% of all information security respondents under management, while another 18% report to the IT department.

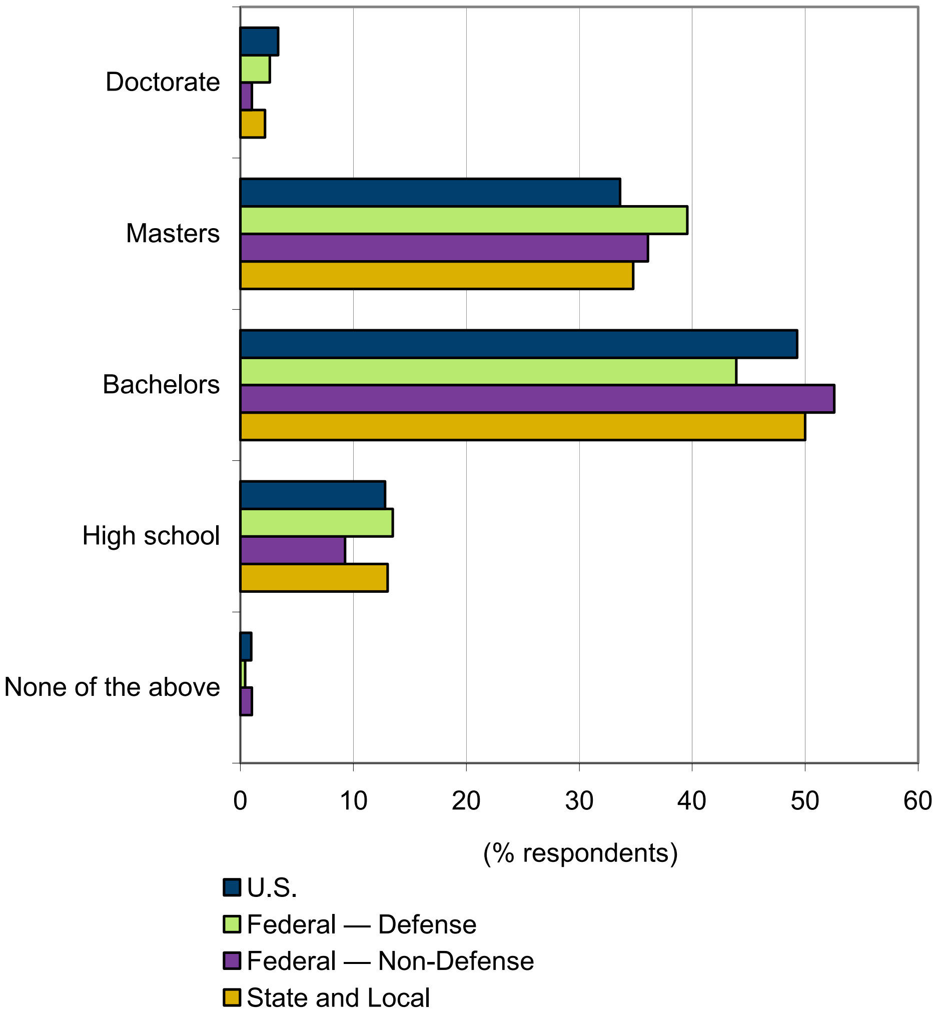
State and Local

Of the respondents employed by a U.S. state or local government, 84% are men and 16% are women. Half of the respondents have bachelor's degrees, while another 35% completed a master's and 2% achieved a doctorate. In aggregate, they have an average of 10.2 years of information security experience and receive $79,709 in salary.

Unlike the U.S. federal government, 46% of S&L information security professionals directly report to their IT departments, significantly more than the 29% reported by respondents in other U.S. industries. The CIO or equivalent executive claimed 26% of all information security respondents in U.S. S&L governments. Only 11% said they report into the security/information assurance group in their organization. This is not a surprising situation given the tremendous IT financial and resource challenges that S&L governments face. These governments often struggle to retain qualified information security professionals and supplement the shortfall by assigning someone in the IT department sole security responsibility or security as a secondary or tertiary function.

FIGURE 4

Highest Level of Education Obtained by Information Security Professionals by U.S. Government Segment



n = 373

Note: U.S. represents all industries except government.

Source: IDC's *Global Information Security Workforce Study*, 2006

TABLE 2

Years of Information Security Experience by Segment (% respondents)

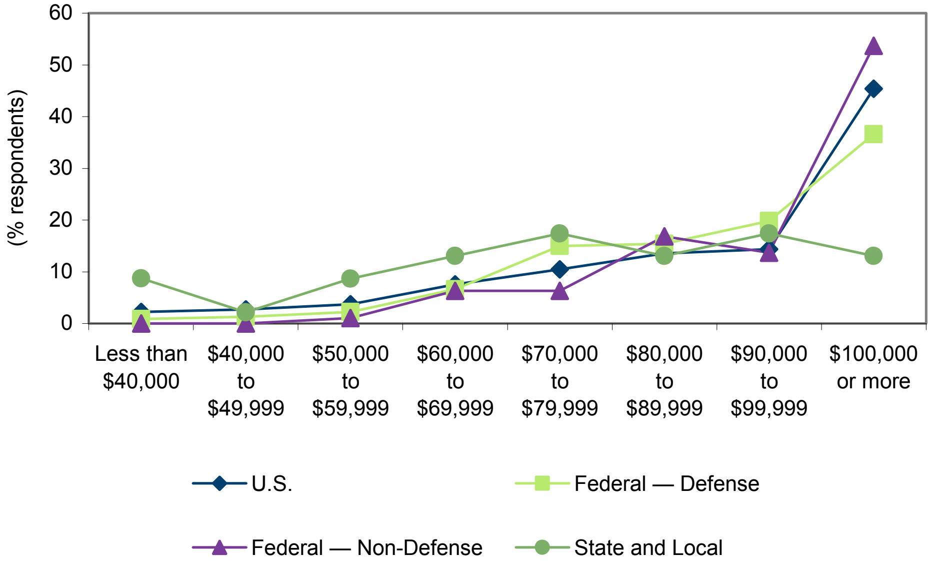
	U.S.	Federal — Defense (U.S. only)	Federal — Non-Defense (U.S. only)	State and Local
Less than 5 years	6.2	6.1	1.0	6.8
5 to less than 10 years	45.2	43.4	41.2	47.7
10 to less than 15 years	23.4	22.4	27.8	15.9
15 or more years	25.3	28.1	29.9	29.5
Average	9.9	10.5	11.2	10.2

Note: U.S. represents all industries except government.

Source: IDC's *Global Information Security Workforce Study*, 2006

FIGURE 5

Salary Bands for Information Security Professionals by Segment ($US)



Note: U.S. represents all industries except government.

Source: IDC's *Global Information Security Workforce Study*, 2006

In general, organizational departments such as risk management, internal auditing, and governance/compliance have been nonexistent in government organizations in the United States, but have become more established in private sector enterprises over the past two years given the escalating regulatory environment globally. That's not to suggest that compliance is not having an impact on how government agencies address their information security challenges. The U.S. federal government does nonetheless have the Government Accountability Office (GAO), which regularly conducts audits and provides recommendations to agencies. The GAO is known for publicly criticizing agencies on their information security efforts and poor FISMA scores in order to prompt reaction and encourage progress. Change can only be properly addressed through human intervention and action — not technology implementation.

Certifications Are Important in Governments Across the United States

In some cases certifications are a condition for employment as a government information security professional. According to 34% of U.S. private sector respondents involved in the hiring process for information security staff, nearly 87% of hiring managers said when making hiring decisions, it is somewhat important or very important that candidates have information security certifications (see Figure 6). Responses from the federal government were much higher. Over 95% of federal information security professionals in the defense sector and over 92% in the non-defense sector said that it is either somewhat important or very important that candidates have information security certifications. Of the 27% of federal-defense government respondents that have hiring influence, the results indicate that certifications are more important to them than their brethren in the private sector, which IDC believes is a direct result of DoD Directive 8570.1. Department of Defense (DoD) Directive 8570.1 requires all DoD information assurance technicians and managers to be trained and certified to a DoD baseline requirement. Thirteen certifications have been identified and approved by the directive's enterprisewide certification program.

On the S&L level, just over 70% of the respondents responsible for hiring decisions said it is either somewhat important or very important that candidates have information security certifications. S&L government hiring managers, which consisted of 37% of the total S&L responses, might not view certifications in the same high regard as their peers in the federal government because they are simply not mandated to ensure their staff carry any one of 13 information security certifications like federal DoD agencies under Directive 8570.1.

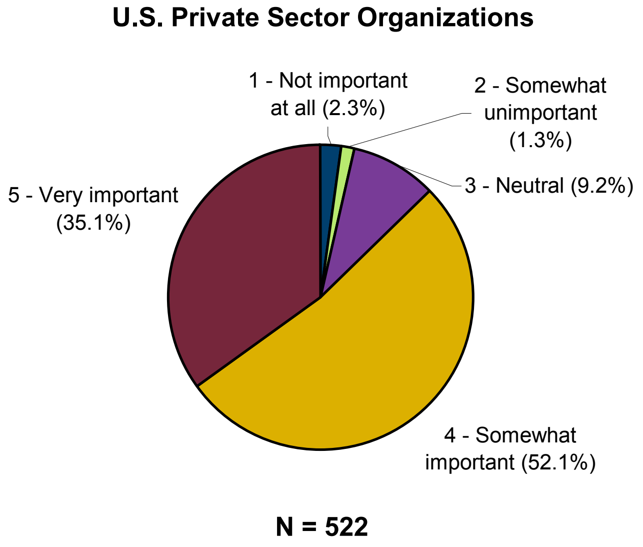
The majority of hiring managers agree that certifications are important in the hiring process. Reasons for requiring employees to acquire information security certifications of employees range from compliance to employee competency for establishing a baseline of knowledge. From the U.S. private sector perspective, the main reason for hiring managers is employee competency as illustrated in Table 3. Almost an equal amount of respondents said their company does not require certifications in order to be hired in information security, which was followed by quality of work at 35% of respondents in U.S. companies. Respondents from the U.S. federal non-defense agencies voiced a similar opinion as the information security professionals in U.S. companies, where employee competency was the top reason and another 40% said it is not required at their organization. On the other hand, almost half of S&L respondents said that certifications in the area of information security are not required by their employer. The other half stated employee competency and quality of work were the two major factors causing their organizations to require certifications.

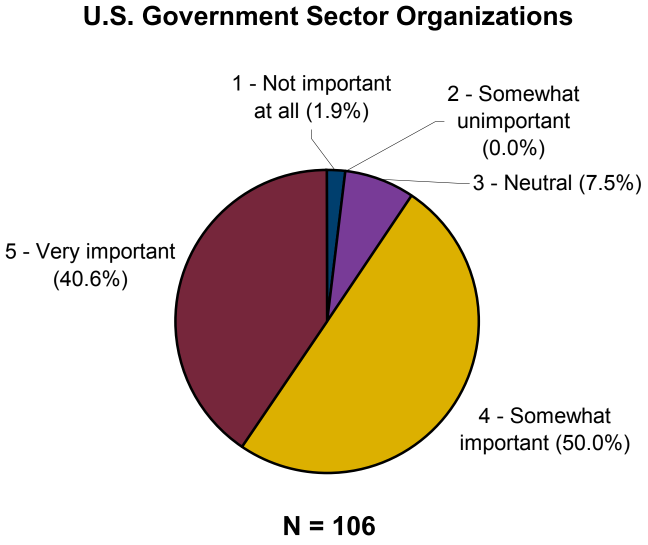
Table 3 also provides evidence as to how much impact DoD Directive 8570.1 has had on respondents working in DoD. Almost 70% said the directive is a main reason for requiring information security certifications, and IDC would expect to see this percentage higher next year as a result of the mandate's progression. Hiring managers are also feeling the pressures of regulatory compliance such as FISMA and want to ensure their information security staffs are knowledgeable, competent and carry the credentials to achieve compliance.

One critical value of certifications is that they establish a foundation from which conscientious professionals can build a common language for professionals to communicate and translate information security requirements from both a strategic and tactical standpoint. Digitally generated threats are continually evolving, and becoming more targeted and sophisticated; as a result, security professionals must equally develop their skills and utilize new tools and techniques to adapt and respond to the threat environment and perpetrators. In some cases, a new certification might be the best approach to validating new skills. Regardless of the certification professionals achieve, their success in the profession will come from their ability to learn new defenses, adapt to changing logical and physical environments, and fully employ and leverage new security tools, techniques, and best practices across infrastructure and the entire organization.

FIGURE 6

Importance of Information Security Certifications When Hiring Information Security Professionals





Note: U.S. represents all industries except government.

Source: IDC's *Global Information Security Workforce Study*, 2006

TABLE 3

Reasons Managers Prefer Hiring Information Security Professionals with Information Security Certifications by Segment (% of respondents)

	U.S.	Federal — Defense (U.S. only)	Federal — Non-Defense (U.S. only)	State and Local
Company policy	20.8	14.2	15.6	15.6
DoD Directive 8570.1	7.0	69.9	11.5	
Employee competence	38.6	31.0	46.9	35.6
Legal/due diligence	15.8	11.9	15.6	17.8
Not required	39.1	16.4	39.6	48.9
Other (specify)	4.4	2.7	4.2	
Quality of work	35.0	21.7	28.1	22.2
Regulatory requirements (governance)	18.5	35.0	30.2	15.6

Notes:

- Multiple responses were allowed.
- U.S. represents all other industries except government.

Source: IDC's *Global Information Security Workforce Study*, 2006

Security practitioners must continue to stay on top of the latest technologies and best practices through continuing education and practical experience to deal with the evolving computing environment (e.g., virtualization, service oriented architecture, and grid computing) and the changing nature of information security. Organizations are cautiously and methodically moving toward a converged security environment in which physical and logical security operate over a single network, but not necessarily operate as a single department or function. Sections of government have been doing this for many years; however, initiatives such as the DoD common access card and, more recently, HSPD-12 are driving standardization across all agencies. Technical knowledge will be important; however, addressing the cultural challenges and utilizing business skills, such as communication, negotiation, and collaboration, will become equally critical to an individual's career advancement and survival in the U.S. government. The need for business skills, in addition to technical skills, is a trend that has been highlighted in all three *GISWS*s and applies to both the private and public sectors.

FUTURE OUTLOOK

C&A and Risk Management Are Key Concerns

U.S. government information security professionals identified additional training and education opportunities across a number of disciplines. Table 4 displays the similarities between the public and private sectors and across U.S. government entities. The top response within the federal government was C&A training, which was the same for defense agencies in 2005. Among non-defense respondents, C&A replaced business continuity and disaster recovery as a top training priority this year. Federal government agencies' C&A performance has received increased attention and oversight by the Office of Management and Budget (OMB). The Expanding

E-Government Scorecard under the President's Management Agenda has established that an agency must certify and accredit 90% of its systems for that agency to receive "green" status on the scorecard. Agencies that achieve 80% compliance receive "yellow" status. In addition, FISMA requires that all federal agencies develop and implement an agencywide information security program designed to safeguard IT assets and data of the respective agency. FISMA provides a framework to ensure comprehensive measures are taken to secure federal information systems and assets. FISMA compliance is mandatory and reported yearly. Hence, federal government employees must be appropriately trained on C&A methodologies and standards to maintain compliance; therefore, information security professionals may seek out additional certifications to qualify and be proficient.

Information security risk management and forensics remain the two top-ranked areas of interest for defense and non-defense, which were consistent with the top two areas for S&L and the private sector. Each area has been a hot topic this year, and IDC believes a trend will continue over the next 12-24 months as organizations struggle to gain control over their risk posture, develop a flexible standards-based framework to quickly and efficiently adapt to new environmental factors such as regulations, and provide visibility into their greatest risks. Previously mentioned in the study, forensics (part of the e-discovery process and a key risk management component) is a hot issue as a result of increased identity theft and data leakage incidents among various U.S. government agencies. Often, public and private sector organizations attempt to remediate after an incident and collect the necessary evidence to prosecute on their own; however, many do not possess the skills at this time and must engage an outside firm to assist in their efforts. Ideally, they would rather keep this in-house and deal with a situation internally, hence the need to train their staff on forensics techniques.

TABLE 4

Top 5 Areas Identified for Additional Training by Segment

Rank	U.S.	Federal — Defense (U.S. only)	Federal — Non-Defense (U.S. only)	State and Local
1	Information security risk management	Certification and accreditation	Certification and accreditation	Information security risk management
2	Forensics	Information security risk management	Information security risk management	Forensics
3	Applications and system development security	Forensics	Forensics	Business continuity and disaster recovery planning
4	Business continuity and disaster recovery planning	Security management practices	Applications and system development security	Access control systems and methodology
5	Security management practices	Access control systems and methodology	Business continuity and disaster recovery planning	Applications and system development security

Note: U.S. represents all industries except government.

Source: IDC's *Global Information Security Workforce Study*, 2006

Some other key areas of interest are applications and systems development security, business continuity and disaster recovery planning, and access control systems and methodology, which rounded out the top five. Application and system development security is a new area of security interest for information security professionals across all U.S. industries with the exception of the DoD. The Department of Defense is not new to application and system development security. As far back as 1970, DoD showed its awareness of application and system development security issues. In that year, the Office of the Director of Defense Research and Engineering for the Defense Science Board's Task Force on Computer Security commissioned a RAND corporation study that resulted in the first attempt to codify computer security — Security Control for Computer Systems (U). In 1984, National Security Decision Directive 145 made the National Security Agency — part of the Department of Defense — responsible for ensuring the security of all classified information transmitted by federal computers.

The rise in attacks, particularly zero-day attacks, against the Web and other critical applications has stirred a movement in the private sector to better understand security's role in application and system development life cycles and post-production environments, which will likely transcend to non-defense agencies and S&L governments. Interest is coming from both information security professionals and software developers alike.

Accountability and Influencing Change in the U.S. Government

Even though C&A and information security risk management are top of mind in the federal government, the individual perceived by respondents to be ultimately responsible for security varies slightly between the U.S. public and private sectors. For information security professionals in U.S. governments, more than 45% believe the CIO or equivalent person is responsible and accountable for maintaining security in the organization as compared to 35% in the private sector. Their perception goes unchanged from what they stated in last year's study where more than 40% believed the CIO or counterpart had ultimate responsibility. What has changed is their perception of the CISO's role and level of accountability for information security. Despite the FISMA legislation mandating that the CIO hold responsibility for federal agency information security, Figure 7 demonstrates that the CISO is believed to be slightly more accountable by government information security professionals than by their peers in the private sector, 16.4% to 14.2% respectively. In 2005, the CISO was the third most-mentioned individual in government and behind the CEO or equivalent. The previously mentioned shift in direct reporting structures and increased attention to security breaches this year could be potential contributors to this changed perception of the CISO within government organizations. Nevertheless, in every other role, management within U.S. private sector organizations shares the risk more broadly than management across U.S. government organizations.

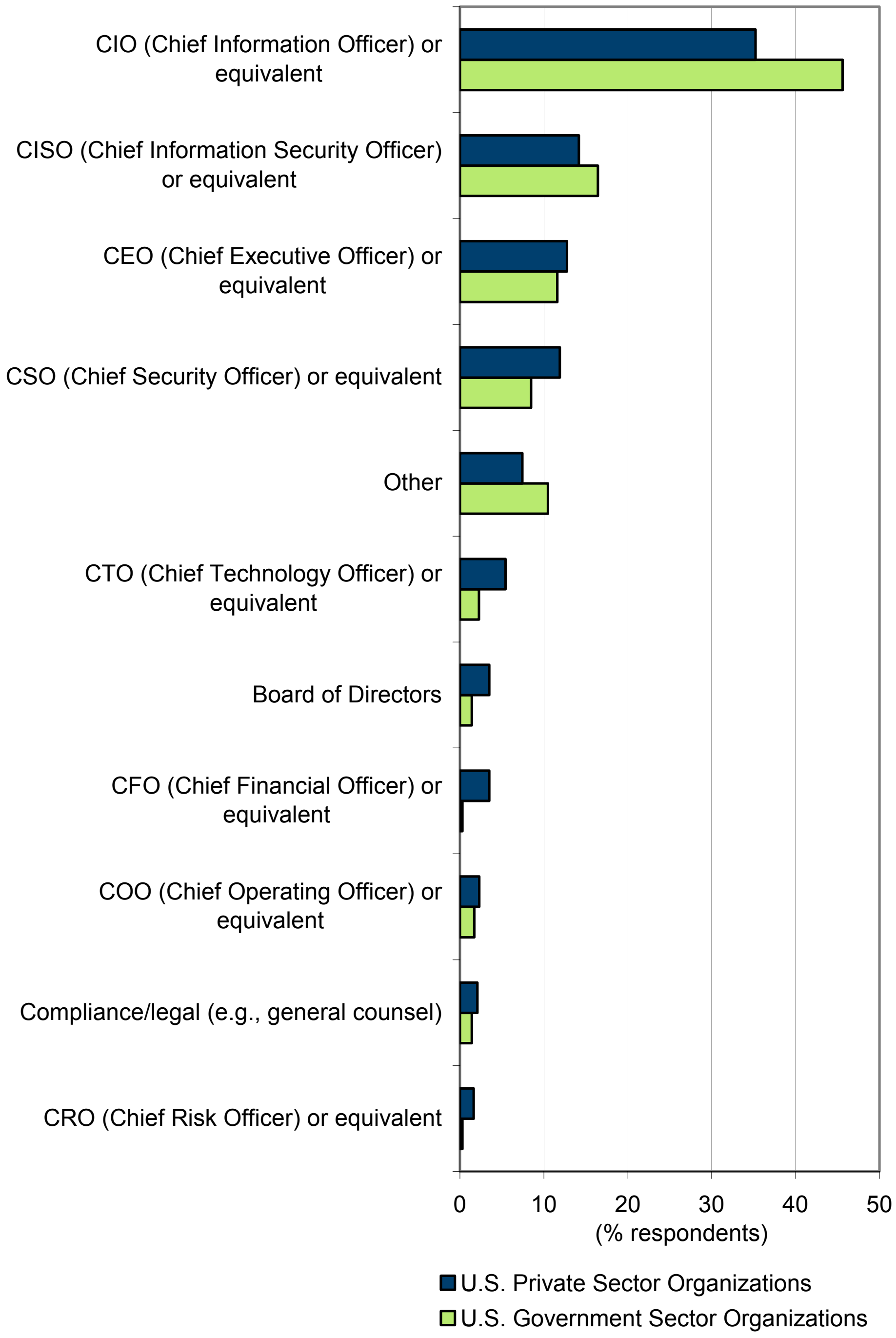
CIOs of government organizations provide vital public services and oversee information and communication systems that support those services. Inclusive of public services is the need for emergency services such as homeland security protection (protecting our nation's critical infrastructure) and first responder assistance and coordination. In the event of a security breach or disaster, government organizations from the federal to the S&L level must coordinate to maintain order and restore essential public services. Government CIOs, therefore, carry the majority of the perceived burden for their IT systems information security. However, the role of the CISO continues to evolve at the federal and S&L levels. This trend for S&L governments was recently highlighted by a National Association of State Chief Information Officers (NASCIO) report released in September 2006. Over time, IDC believes CISOs will be better positioned to drive governmentwide awareness and promote interagency cooperation on information security efforts to meet the demands of directives such as Homeland Security Presidential Directive 7 (HSPD-7).

In the U.S. private sector, CIOs and CISOs are already sharing the accountability for information security but to a lesser extent than government because other members of their management teams, including the CEO and CSO, are perceived to be ultimately responsible. Accountability sharing within private sector organizations stretches beyond the management team to the board members, chief technology officer, and the chief risk or compliance officer. The private sector takes more of a distributed approach to risk management, which causes employees to identify a variety of individuals as being ultimately responsible for information security. In the public sector, roles and responsibilities are clearly, defined, structured, and communicated amongst the rank and file, so there is no confusion as to who is responsible for what area or discipline.

Despite the challenges of illustrating the value of information security and attaining the appropriate level of funding to mitigate the acceptable level of risk, information security professionals have remained positive about their ability to influence management and have been instrumental in changing the mindset of management and gaining their buy-in that information security is an organizationwide priority. During the past 12 months, 69% of government security practitioners in the United States believe their efforts were effective in bringing change to their organizations. Their efforts have also been assisted by government mandates and media coverage of high-profile incidents. Thinking ahead to 2007, 75% of government information security professionals remain optimistic that they will be able to influence management and organizational stakeholders to drive security awareness and responsibility. In comparison, government security practitioners are more optimistic about their ability to cause change than the 70% respondents in U.S. private sector organizations.

FIGURE 7

Individual with Ultimate Accountability for Organization's Information Security Functions



Note: U.S. represents all industries except government.

Source: IDC's *Global Information Security Workforce Study*, 2006

For information security professionals across government and all other U.S. industries, relationship building and gaining consensus will be key initiatives in the coming year as they strive to build support for information security policies that are typically set forth by the CSO or CISO. Regulatory compliance is helping the situation, but U.S. information security professionals need to persuade management in order to sustain their momentum for creating change among stakeholders. According to U.S. government respondents across federal and S&L, management's support of security policies is a security practitioner's primary concern for effectively securing their organization's infrastructures. The following list shows the elements (in ranking order from most important to least important) affecting information security professionals' ability to properly protect and secure the computing infrastructure and its resources from breaches, misuse, and abuse:

1. Management support of security policies
2. Users following security policy
3. Qualified security staff
4. Software solutions
5. Hardware solutions

Based on this year's results, the top three highlight the need to focus more time and attention on policies, processes, and people — areas that can no longer be overlooked and are being addressed through a variety of vehicles, including mandates and directives. One difference in the ranking to note is that DoD respondents believe that users following security policy and having qualified security staff are equally important to properly securing their organizations' operations. Consequently, information security professionals in the U.S. public sector have shared their understanding of the challenge — how to better manage security risk - and identified what needs to be done in order to better protect our nation's critical infrastructure and public services. The task at hand is communicating the needed resources and associated solutions to execute a sound security strategy and support a well-defined and well-articulated risk management program where everyone acknowledges their role in organizational security and acts responsibly.

CONCLUSION

U.S. government officials from the executive branch down through the chain of command recognize information security is a global, governmentwide priority. The fact remains that information security cannot be addressed through the sole use of technology solutions. The unwavering commitment of the U.S. government is required at the financial, management, and operational levels to proactively secure and protect the nation's logical and physical assets. Effective security management requires the dynamic balance between people, policies, processes, and technology to effectively mitigate the risks associated with being digitally connected and participating in an information-sharing, intelligence-driven environment.

IDC believes that the 373 information security professionals from U.S. public sector organizations who shared their views and opinions in this study are well educated and experienced professionals that take information security and risk management seriously because our nation's critical infrastructure and citizen services depend upon their skills and abilities to defend against malicious hacking, identity theft, and cyber warfare. Even though demonstrable security value continues to be a challenge to justify, the significance of people, policies, and processes as an essential triad for effective, proactive information security is finally resonating in government organizations. Derived from the study results, IDC advises government information security professionals in the United States to consider the following conclusions:

- Certifications are an increasingly important criteria for not only hiring but also for career advancement of younger employees, particularly in U.S. federal government. Continuing education will play an equal important role in staying on top of the trends, threats, and best practices, and will provide an opportunity for specialization.

- Gaining management support of information security policies, educating end users, and enforcing those policies will be significant challenges for 2007, but peers in the public sector are optimistic on their chances of influencing change.

- Compliance directed at U.S. government organizations continues to invoke organizational changes, such as mandating information security certifications, stricter policy enforcement, and better information protection frameworks.

- Information security professionals remain in high demand within the U.S. government, particularly those with certifications, qualified experience, and management skills. Opportunities for specialization exist in the areas of C&A, audit, and forensics.

- Security domains such as C&A, information risk management, forensics, and application and systems development security are education topics where information security professionals and managers are looking for more training and knowledge.

Copyright Notice