

## WHITE PAPER

---

### 2006 Global Information Security Workforce Study

---

Sponsored by: (ISC)2

---

Allan Carey  
October 2006

#### IDC OPINION

Securing an organization's information assets is a relentless battle. The constant barrage of threats keeps information security professionals in a reactive mode. Cybercriminals are generating attacks using a growing arsenal of weapons, including spam, phishing, malware, and spyware; however, the intent of malicious activity has clearly shifted away from notoriety toward profit. According to various threat reports, more zero-day attacks are surfacing than ever before, further highlighting the need for executives to gain broad visibility across the organization and develop a proactive security strategy.

The formulation of a security strategy also requires people and processes to be addressed as they, too, are significant areas for exposure. If overlooked, intentional and unintentional behavior of users, social engineering, lack of business continuity planning, or insufficient separation of duties can all lead to serious consequences. Organizations must evaluate all internal and external risks on both physical and logical levels to properly execute against their risk management objectives.

External and internal threats leave little time for information security professionals to research new technologies and review policies and processes to get ahead of the security problems. Executive buy-in, end-user awareness, and information security staff competencies continue to be challenging areas for security practitioners as they balance their time between IT and business. This balance will play a crucial role moving forward as information security professionals become a vital link to their organizations' success, a trend that has continued over the past three years.

This study is designed to reflect the opinions of today's security workforce and provide a glimpse into the future of the information security profession. IDC believes the following factors will keep information security high on the organizations' priority list for the foreseeable future:

- Increasing regulatory compliance within the public and private sectors requires strong security policies, processes, and controls, which will force organizations to adopt security standards and frameworks for a long-term approach to mitigating risk.
- Evolving and emerging threats and attacks will continue to require security professionals to learn new skills and techniques.
- Accountability between information security professionals and management falls on several key executives to manage growing risk exposures.
- Both physical and logical securities are at risk, which means that security is now everyone's responsibility within the organization.

## EXECUTIVE SUMMARY

On behalf of the International Information Systems Security Certification Consortium (ISC)<sup>2</sup>, IDC was engaged 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 4,016 respondents from companies and public sector organizations around the globe 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 are:

- ☒ The number of information security professionals worldwide in 2006 is estimated to be 1.5 million, an 8.1% increase over 2005.
- ☒ Executives and board members are sharing in the accountability for information security and overall risk management. Twenty-four percent (24%) of CISOs/CSOs have accountability, while the CIO is accountable 3 out of 10 times, and legal, head of compliance, and risk officer roles are evolving and taking on more responsibility.
- ☒ Policy, process, and people are key factors that need significant attention for organizations to effectively secure their computing environments.
- ☒ On average, more than 41% of information security budgets is spent on personnel, including salaries and benefits, and education and training.
- ☒ Employee competency and quality of work remain the top reasons that employers and hiring managers continue to place emphasis on security certifications. Company policy and regulations are becoming critical reasons as well.
- ☒ Security professionals are asking for additional education and training in the areas of information risk management, business continuity/disaster recovery planning, and forensics.

Successful professionals must take the initiative to keep current on key security issues each and every day. A regimen of continuing education and challenging assignments offering exposure to new parts of a business or new responsibilities is sure to have a positive effect on any security practitioner's career development. With the unconditional commitment of an organization at the financial, management, and operational levels, knowledgeable and qualified information security staff can collaborate with security-aware end users to proactively secure and protect the information, financial, logical, and physical assets. Security management will always require striking the appropriate balance between people, policies, processes, and technology to cost-effectively mitigate risk.

## METHODOLOGY

The 2006 *Global Information Security Workforce Study (GISWS)* was conducted during the summer of 2006 on behalf of (ISC)<sup>2</sup>, a nonprofit organization dedicated to providing education, certification, and peer-networking opportunities for information security professionals worldwide. (ISC)<sup>2</sup> 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)<sup>2</sup> 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 and private organizations; therefore, the results should not be projected across the entire population at large. The data points are meant to be interpreted as leading market indicators and reflect the opinions of the 4,016 individuals surveyed for this IDC study.

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

## SITUATION OVERVIEW

---

### Introduction

Identity theft, lost or stolen laptops, tapes being misplaced or falling off the backs of trucks, and other incidents that threaten the integrity and confidentiality of business information have kept information security in the headlines over the past year. Aside from the daily hacker and vulnerability news, events such as these are highlighting the need for better data protection strategies and better oversight of those bestowed with custodianship of data. Compliance requirements from regulations such as the Payment Card Industry (PCI) Data Security Standard, Sarbanes-Oxley, Federal Information Security Management Act (FISMA), and Basel II are fueling the demand for information security solutions and qualified staff to architect, deploy, and manage the solutions, including the people, policies, and processes controlling them. However, the demand for individuals who interpret, advise, and implement solutions, generating large volumes of reports for auditors, will not last into perpetuity. As compliance infrastructures and processes are put into place, many of the personnel will eventually be reassigned to different roles and responsibilities.

Security professionals have done a commendable job of raising awareness of security issues within their own organizations and remain positive about their ability to influence management and, consequently, future security decisions. Although information security professionals have made great strides over the past year, more work still needs to be done. External and internal perpetrators continue to drive malicious activity, and both attackers and legitimate "white hat" security researchers are broadening their scope and targeting many types of security solutions, including security hardware, software, and managed services. In response, enterprises must be vigilant and strengthen their internal access controls, improve visibility across the network, and enhance security policies, processes, and procedures. Furthermore, the technology solutions alone will not be sufficient without qualified personnel who are able to set policy and configure and implement technology-based solutions according to best practices and standards.

Accordingly, the increased demand for qualified information security professionals among organizations, particularly those with more than 1,000 employees, and the market demand for such individuals with both technical and business skills continues to grow. Common sense would dictate that as greater resources are allocated to an enterprise security budget, executives would increase the size of their staff dedicated to enterprise security and better inform employees through training and awareness to avert human error. Today, this is not always the case. Management of organizations typically prefer to minimize overhead increases and maximize the integration of existing technology investments to further extract value such as enhanced visibility, improved operational performance, and greater reliability. To compensate for limited resources and internal capabilities, organizations often choose to engage with a third-party services firm that has been able to attract qualified information security professionals. However, providers of security services are also challenged to find appropriate candidates for vacancies within their security workforces. For those reasons, opportunities prevail for individuals with a combination of training and hands-on experience in information security and skills in business.

The factors driving growth in the profession are similar this year to those from 2005, with government regulations, an escalating and more targeted threat environment, and dynamic business operations being contributing factors for growth in the demand for information security professionals. As many of us know, increasing headcount does not always solve problems, especially when financial hurdles are put in place to challenge hiring justifications. Ideally, finding qualified individuals with specialized expertise in the information security field will yield better results. Should the right candidates not be available, organizations are compromising by relying on junior-level individuals to fill the void in the employment pool. By staffing with less qualified individuals, organizations are making the conscious investment to train and educate employees so that over time they can attain an acceptable level of knowledge and capability. Regardless of employees' age and experience, continuing education and training are essential to staying ahead and having the most up-to-date knowledge to properly protect the enterprise. Consequently, the demand for information security professionals over the next five years will be influenced by a number of factors:

- ☒ **Budgets.** Information security managers are constantly challenged to justify their needs and priorities and to align spending with business objectives such as contributing to top-line revenue or operational cost savings.
- ☒ **Compliance.** Information security has moved further up the corporate agenda as executives try to stay off the front page of the newspaper. Significant consulting and technology costs are causing management to seek methods of automation to demonstrate due diligence and, thus, compliance.
- ☒ **Third-party services.** Security service providers are being increasingly asked to provide staff augmentation services because the cost of attracting, hiring, and retaining top talent is an expensive value proposition. For many organizations, security is not a core competency.

IDC estimates the number of information security professionals worldwide in 2006 to be approximately 1.5 million, an 8.1% increase over 2005. This figure is expected to increase to slightly more than 2 million by 2010, displaying a compound annual growth rate (CAGR) of 7.8% from 2005 to 2010 (see Table 1). The Asia/Pacific and Europe, the Middle East, and Africa (EMEA) regions will present higher growth opportunities for information security professionals than the Americas. Organizations in both regions are developing compelling propositions to entice qualified practitioners such as Australia's Migration Occupations in Demand List (MODL), which includes information security professionals. Besides, Asia/Pacific and EMEA tend to lag the United States by approximately 18 months when it comes to information security market maturity; therefore, these regions are now experiencing above-average growth that occurred in the United States four to five years ago, which is a significant factor in the CAGR decrease over the past two years. Table 1 reflects these findings from our observations of staffing behavior during the previous 12 months and from our primary research on organizations' intentions to increase their information security budgets, including staffing.

The forecast presented in this study represents IDC's best estimates and projections for 2005–2010 based on reported and observed trends and events in 2005, such as worldwide and regional economic growth will remain flat and company profits in 2006 will be less than 2005's 15% growth but still positive, and their predicted impact on the particular market for the five-year period. Predictions can be influenced by future segment-specific developments, including the anticipated impacts of customer behavior, supplier actions, market competition, and relevant changes in the regulatory environment.

**TABLE 1****Worldwide Information Security Professionals by Region, 2005–2010**

	2005	2006	2007	2008	2009	2010	2005–2006 Growth (%)	2005–2010 CAGR (%)
Americas	606,268	640,705	685,877	727,937	771,432	825,201	5.7	6.4
EMEA	348,162	379,142	407,917	437,463	467,386	499,962	8.9	7.5
Asia/Pacific	458,844	507,261	566,100	627,098	686,120	733,943	10.6	9.8
Total	1,413,273	1,527,107	1,659,893	1,792,498	1,924,938	2,059,106	8.1	7.8

**Notes:**

- Growth in the number of IT employees globally will be 4.6% during the forecast period.
- Macroeconomic changes in the future will have a positive or negative effect on this forecast.
- Unemployment worldwide will stay about the same in 2006 as 2005 levels.
- The United States will remain a leader in adopting advanced security solutions.
- Asia/Pacific will remain a key growth region for information technology and outsourcing.
- Security staffing requirements vary depending on company size, business model, industry, and IT budget.
- Interest in gaining information security specialization by IT professionals and newcomers will continue throughout the forecast period.
- Government, academia, and the private sector will promote programs to attract new talent to the information security profession.
- Internal staff dedicated to security activities will always be required.
- Individuals encompassed within the forecast include full-time and part-time information security professionals, practitioners, and other employees across a multitude of job titles.

Source: IDC, 2006

**Study Demographics**

This year's study reached a broad cross-section of information security professionals in more than 100 countries. Respondents came from the three major regions of the world: Americas (57.3%), EMEA (22.8%), and Asia/Pacific (including Japan) (19.5%). The sample population is a more geographically diverse representation than in past years when the Americas constituted more than 70% of respondents.

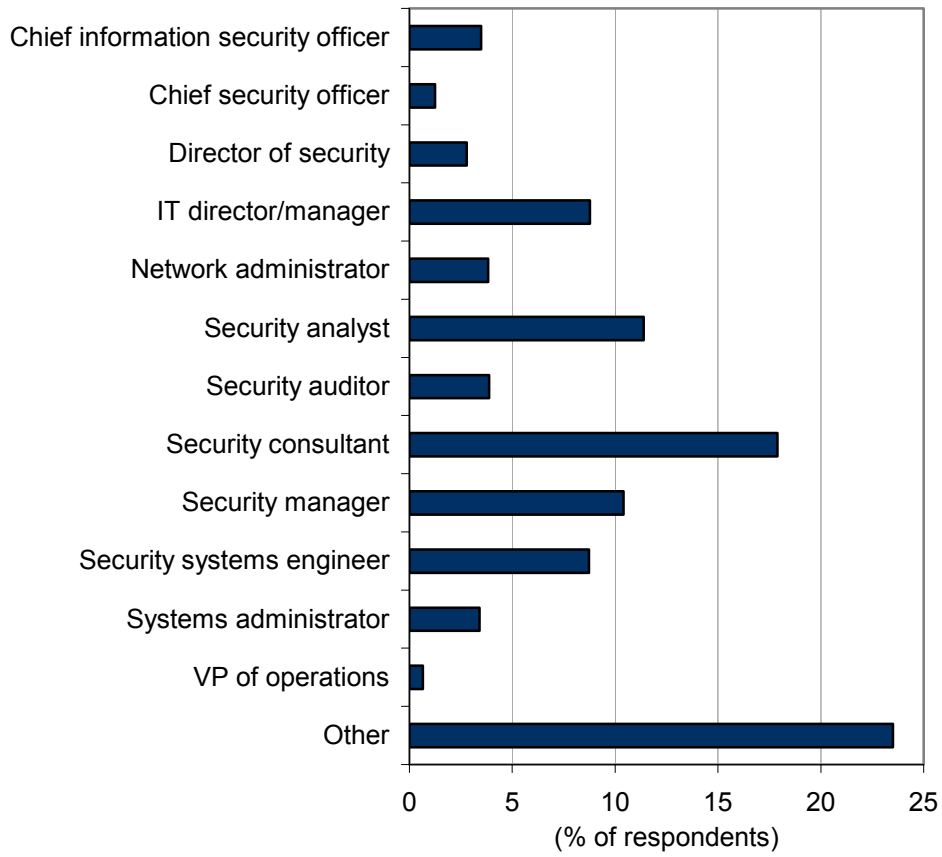
Security professionals who participated in the survey spanned a multitude of job functions and titles, ranging from security analyst to chief security officer (CSO). Figure 1 shows that approximately 5% were at the executive level, while the remainder were at least a security engineer or higher within their organizations. Less than two-fifths were security consultants who either own their own business or are employed to advise clients. Each respondent is involved, in some capacity, in information security decisions, ranging from technology selection to security management to hiring staff. Individuals with sole responsibility for physical security were not included in this study.

Information security professionals surveyed this year represent organizations of all sizes. Very large enterprises and organizations (10,000+ employees) accounted for 4 out of 10 respondents. Approximately 23% are employed by organizations with more than 1,000 but less than 10,000 employees, while 14.5% are from companies with 99 employees or fewer. Midmarket or medium-sized organizations accounted for the remaining 16% (see Figure 2). Annual revenue was another criterion measured to gain a different perspective on the types of organizations employing information security professionals. A total of 3 out of 10 organizations generate between \$1 billion and \$50 billion in revenue annually. Those with less than \$100 million in annual revenue comprised 27% of the respondents (see Figure 3).

Information technology, financial services, government, and professional services accounted for the top 4 industries (see Figure 4). This is consistent with the vertical breakdown in the 2005 *G/SWS*. Many of the organizations face security challenges similar to those they faced last year; however, the methods and means employed to mitigate risk vary greatly across different industries. Regulatory mandates and varying access to resources such as capital and staff force each industry and size of organization to address their information security needs with the right balance of risk versus cost. Each organization is not willing to accept the same level of risk as another and must evaluate how much it is willing to spend to achieve the acceptable risk level.

**FIGURE 1**

Respondents by Job Title or Function



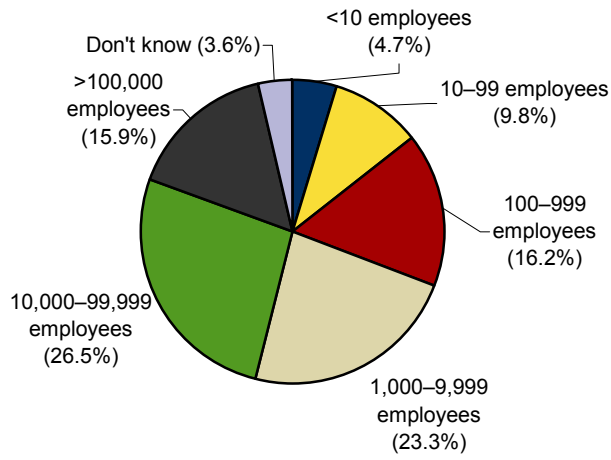
n = 4,016

Note: "Other" represents titles such as information assurance officer, consultant, and security architect.

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

**FIGURE 2**

Respondents by Organization Size

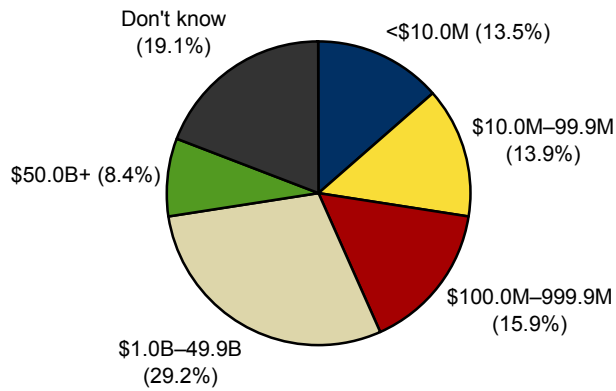


**n = 3,610**

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

**FIGURE 3**

Respondents by Company Revenue/Organization Budget

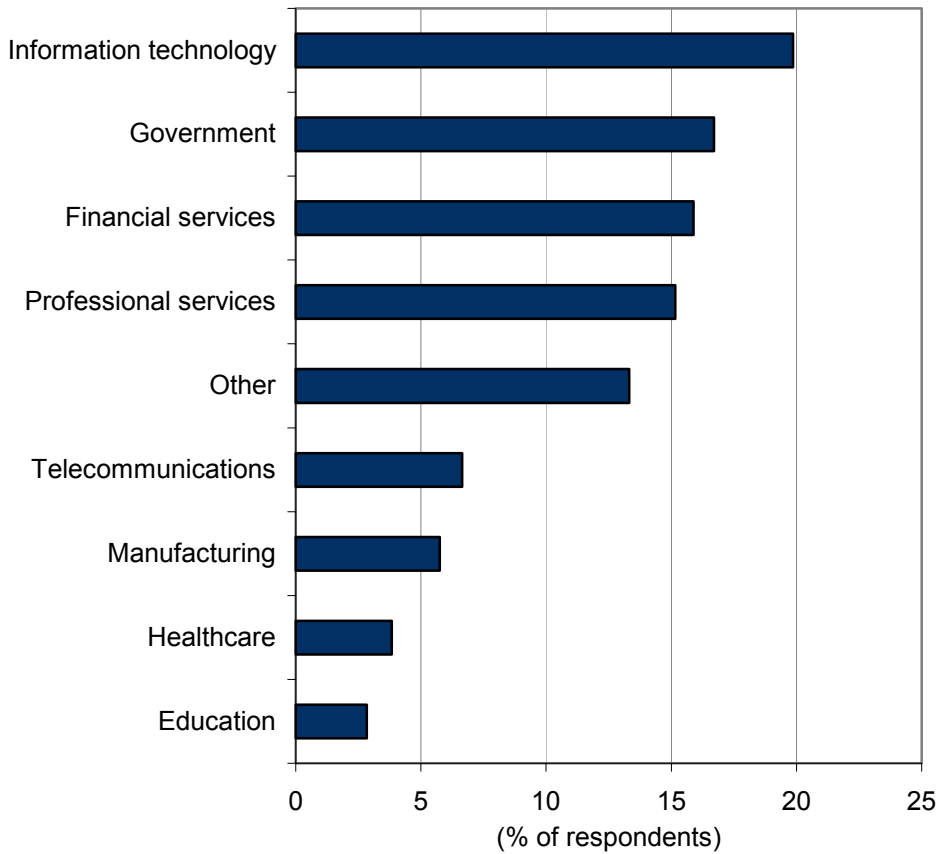


**n = 3,108**

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

**FIGURE 4**

Respondents by Vertical Industry



n = 4,016

Note: "Other" represents industries such as construction, media, and retail.

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

**Accomplishing Near-Term Goals**

Research conducted by information security professionals has resulted in recommendations and investments in some advanced security solution areas to enhance their organizations' risk management capabilities. Table 2 emphasizes the top 5 security areas/solutions being deployed within each region. Some common security technology areas being implemented by organizations across the regions are biometrics, wireless security, intrusion prevention, and forensics tools. As in 2005, wireless security abounds as a security problem that needs to be locked down and controlled. The proliferation of mobile devices, users wanting ubiquitous access, and the increasing mobility of the global workforce create a situation of risk and vulnerability whereby organizations are having a hard time controlling and managing their IT environments.

Surprisingly, biometrics was mentioned as number 1 or number 2 across all the regions. Based on other IDC research, the most common applications for biometrics are physical access and an additional layer of strong authentication for IT systems access. In addition, biometrics are being leveraged as an additional credential that is then linked to an individual's identity for verification purposes (e.g., epassports and national identity cards).

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 enterprise IT staffs, 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 organization's computer systems. Increasing scrutiny of IT systems brought about by new government/industry regulations and best practices has reignited the interest in and demand for security investigation and cyberforensics capabilities.

In the Americas and EMEA, business continuity and disaster recovery has dropped off the top 5 list this year. Priorities have also shifted in EMEA and Asia/Pacific, moving away from identity access management to the same top 3: wireless, biometrics, and forensics.

To achieve successful completion of these security projects, organizations are spending more than 41% of their security budgets, on average, on personnel and staff training to support postdeployment management. Overall, organizations are spending a greater percentage of their information security budgets on personnel and training in 2006 than last 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.

Figure 5 highlights regional differences in funding security staffing requirements. The spending level in the Americas region, which is predominantly influenced by the United States, is slightly higher than the worldwide average due to the higher cost of labor. Asia/Pacific-based organizations spend slightly less than their counterparts in other regions of the world, but are spending more in 2006 than they did in 2005. Changes in the supply/demand model in EMEA, particularly Western Europe, are causing employers to increase their personnel and training budgets by an average of 5%. Qualified individuals are in high demand as seen in Table 1 and, therefore, commanding higher salaries. If qualified individuals are not available or organizations are not willing to pay the premiums, they are opting for lesser-qualified individuals and are investing in training and education to get them up to speed. Throughout Central and South America and Central Europe, the Middle East, and Africa (CEMEA), the average organization spends less on all aspects of IT security than elsewhere in the world.

Anticipating the next 12 months of security projects and gaps in security skills, half of information security professionals believe staffing levels will remain the same (see Figure 6). This sentiment aligns with other IDC research in which enterprises have stated they are requiring IT security departments to do more with the same resources.

Another 45% of respondents indicated they expect an increase in spending on personnel. Further supporting their optimism, when IDC asked security influencers in the fall of 2005 where they would allocate the dollars if they had more budget (see *Enterprise Security Survey, 2005*, IDC #34561, December 2005), enterprises with more than 1,000 employees stated they would increase internal security staff and/or better train employees to avert human error.

Similar to their beliefs regarding spending on staffing, more than half of security professionals believe spending on training will remain the same this coming year. For the 39% of individuals across the regions expecting to see an increase in training spending, they anticipated an average 30% uplift for 2007. In comparison to 2005, 9% more information security professionals are optimistic about seeing an increase in training expenditures in 2007 over 2006.

In the short term, we can expect to see an increase in initiatives that are designed to securely enable mobility and manage risk more effectively. Information security professionals will be instrumental in advising, deploying, and managing these efforts as they align with the business objectives. They will be successful only if armed with the appropriate resources and skills and backed by senior management.

**TABLE 2**

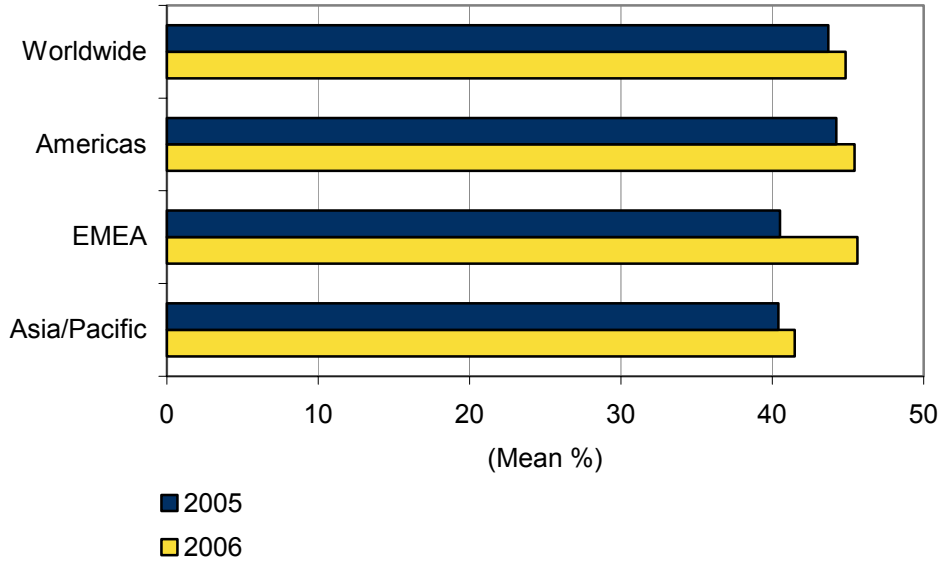
Top 5 Security Technologies Being Deployed by Region

Rank	Americas	EMEA	Asia/Pacific
1	Biometrics	Wireless security solutions	Wireless security solutions
2	Intrusion prevention	Biometrics	Biometrics
3	Wireless security solutions	Forensics	Forensics
4	Identity and access management	Intrusion prevention	Storage security
5	Security event or information management	Risk management solutions	Business continuity and disaster recovery solutions

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

**FIGURE 5**

Share of IT Security Budget for Personnel and Training,  
2005 and 2006

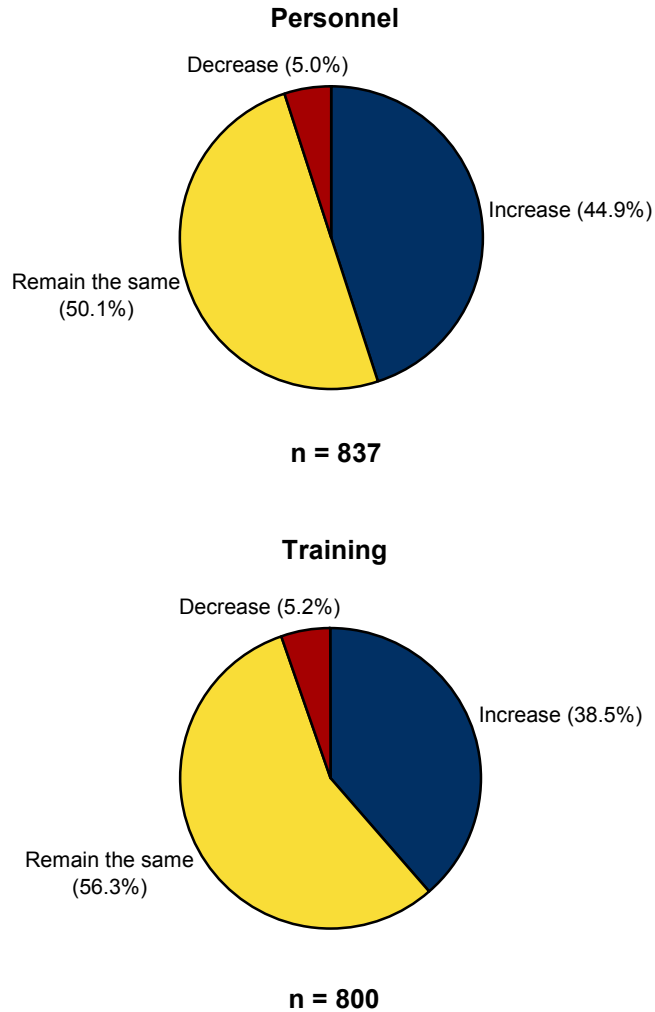


Note: Values shown represent the average across company size within the region.

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

**FIGURE 6**

Expected Change in Budget for IT Security Spending by Category in the Next 12 Months



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

### **Profile: The Information Security Professional**

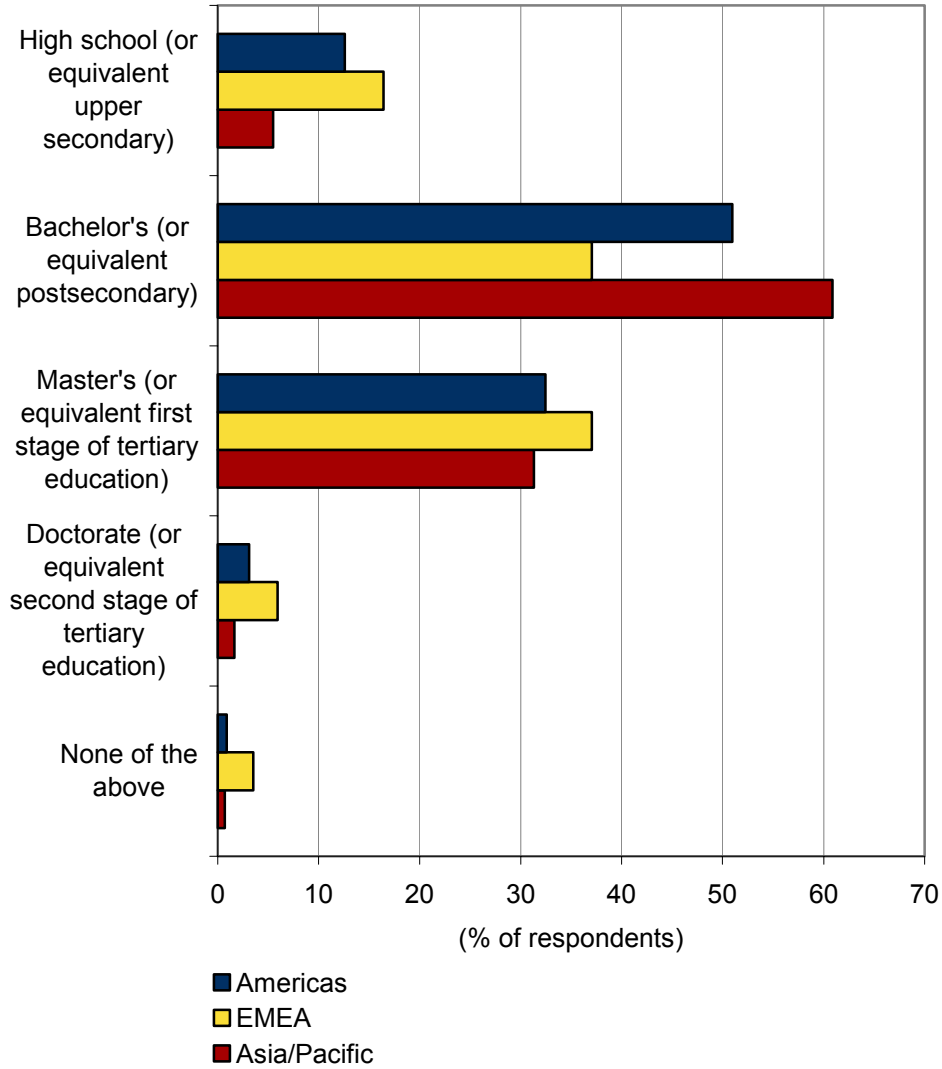
Men and women alike expressed their opinions in this year's *G/SWS*. Compared with the past two years, slightly more women were represented — 13% in 2006 versus 10% in 2005 and 11% in 2004. Six out of ten women were employed in the United States, with excellent representation across Canada and the CEMEA regions (10% and 11%, respectively). Central and South America, Western Europe, and Asia/Pacific security workforces continue to consist of more than 90% men.

From a professional development viewpoint, respondents again reported achieving a high level of education (see Figure 7). More individuals with at least a bachelor's degree or equivalent are employed in the information security workforce. At the bachelor's level, the Americas and Asia/Pacific illustrated an increase over last year (2% and 4%, respectively). EMEA displayed no change in equivalent postsecondary population based on the International Standard Classification of Education (ISCED); however, fewer information security professionals carrying equivalent first-stage tertiary education were represented, 42% in 2005 versus 37% in 2006, which remains an improvement over the 32% reported in 2004. Within the Americas, the number of individuals holding a master's degree decreased slightly from 35% to 32%, with 32% being an improvement over the 28% reported in 2004. Doctorate-level (or equivalent second stage of tertiary education) status was reported by 3.5% of information security professionals worldwide, which is unchanged from 2005 and slightly up by 1% from the information security community during 2004. Nearly 9% of Western European respondents reported having a doctorate-level degree, more than any other region on a percentage basis.

Years of professional experience proved to be another important candidate criterion for hiring managers and their organizations as a complement to or substitute for education (see Table 3). With a maturing workforce and new entrants fulfilling the staffing needs in organizations, some shifts have occurred across reported experience segments. In 2004, the average security professional across each region had been in the industry for 8 years (Americas), 6 years (EMEA), and 5 years (Asia/Pacific). In 2006, security professionals in the Americas averaged 9.6 years of experience, while security professionals in EMEA and Asia/Pacific averaged 7.7 years and 7 years, respectively.

**FIGURE 7**

Highest Level of Education Obtained by Information Security Professionals by Region



n = 3,867

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

**TABLE 3**

Years of Experience of Information Security Professionals by Region,  
2005 and 2006 (% of Respondents)

	Worldwide		Americas		EMEA		Asia/Pacific	
	2005	2006	2005	2006	2005	2006	2005	2006
Less than 5 years	12.3	16.7	9.6	12.6	12.5	18.8	23.2	26.3
5 to less than 10 years	47.7	48.5	43.8	46.0	53.6	54.1	59.1	49.6
10 to less than 15 years	20.4	20.8	21.9	22.5	21.9	19.2	12.7	17.7
15 or more years	19.6	14.0	24.7	18.8	12.0	8.0	5.0	6.3

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

Most noticeably in EMEA, the segment with less than five years of information security experience grew by more than 6% over 2005. In 2006, the Americas and Asia/Pacific saw a similar increase of approximately 3% in the same segment of the workforce. On the other hand, Asia/Pacific experienced a visible 10% decline to 49.6% for individuals with 5 to 10 years of experience, and as a result, security practitioners with 10 to 15 years of experience increased to 17.7% and the remaining 5% was distributed across the other experience segments. A decrease in the percentage of information security respondents with more than 15 years of experience was observed in the Americas and EMEA as some of the distribution moved toward the group with less than 10 years in a security capacity. This is not to imply that individuals within the information security workforce have rapidly aged and retired over the past year. It does mean more individuals are entering the workforce with less experience, causing a shift in the distribution across the experience segments.

With more individuals achieving higher education levels and gaining valuable experience, information security salaries this year have shifted globally to reflect some of the regional dynamics taking place. In the Americas, the percentage of individuals reporting salaries under \$30,000 increased by 3% to 4.4% of the workforce, which was the most notable change among Americas-based respondents (see Figure 8). The shift is mainly due to an increase in the number of information security professionals being employed in Central and South America at salaries that are lower than average for the region.

The EMEA marketplace, however, experienced a more dramatic change in the same salary range. Figure 9 shows that 14% of security practitioners earned less than \$30,000 in 2006 compared with 5.6% in 2005 and 1.5% in 2004. Organizations in EMEA, particularly Western Europe, are struggling to find qualified candidates, and those who are available are commanding higher salaries. Organizations not willing to pay higher salaries are resorting to hiring less qualified individuals with either insufficient experience and/or inadequate skills and subsequently having to invest in training, education, and/or certifications. As a result, the 2006 salary trend for information security professionals across EMEA is rebalancing to compensate for the influx of less experienced, lower-paid security staff, which is causing employers to increase the personnel and training portion of their IT security budgets.

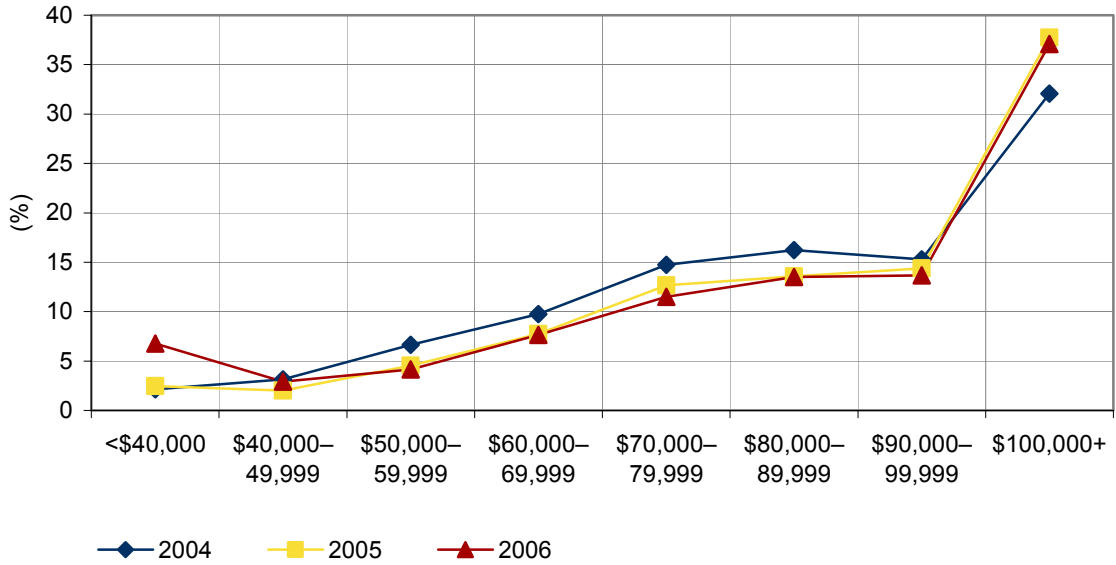
Asia/Pacific salaries have progressed and are starting to come in line with those in other regions of the world (see Figure 10). For individuals earning between \$70,000 and \$125,000, there was a 6.2% positive difference over 2005. On the lower end of the spectrum, security professionals in Asia/Pacific earning less than \$40,000 still make up more than 39% of all respondents in the region. This is 7% less than last year, which was on par with 2004.

Reporting lines for the majority of information security professionals worldwide have not changed dramatically over the course of the past 12 months. Three out of every ten still directly report into the IT department, which is slightly less than the 32% reported in 2004 and 2005. The security department/information assurance group claimed 20% of all information security respondents, which remains consistent with the results from 2005 and exceeds executive management by 2% this year. Other groups such as risk management, internal auditing, and governance/compliance have become more established in organizational hierarchies over the past two years given the escalating regulatory environment globally. Jointly, 8% of all responding information security professionals report directly to these groups.

According to this year's results, the information security workforce is experiencing growth in the number of practitioners with less experience and insufficient skills, particularly in EMEA and Asia/Pacific. The majority have at least a bachelor's degree (or equivalent education) but will require the mentoring of more established security professionals, in addition to education and training, to advance their careers and ascend the organizational ladder.

**FIGURE 8**

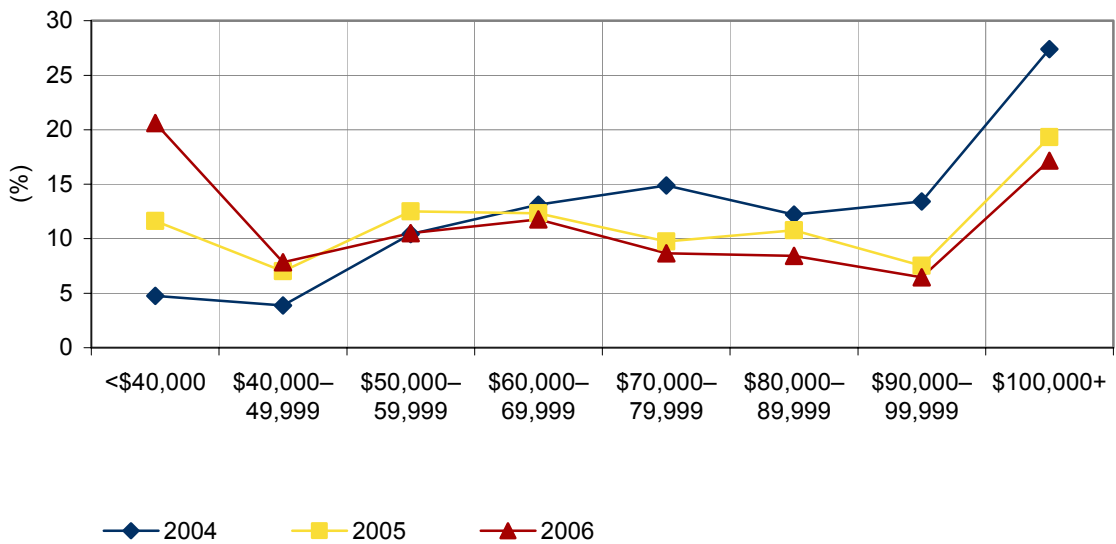
Americas Salary Bands for Information Security Professionals, 2004–2006



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

**FIGURE 9**

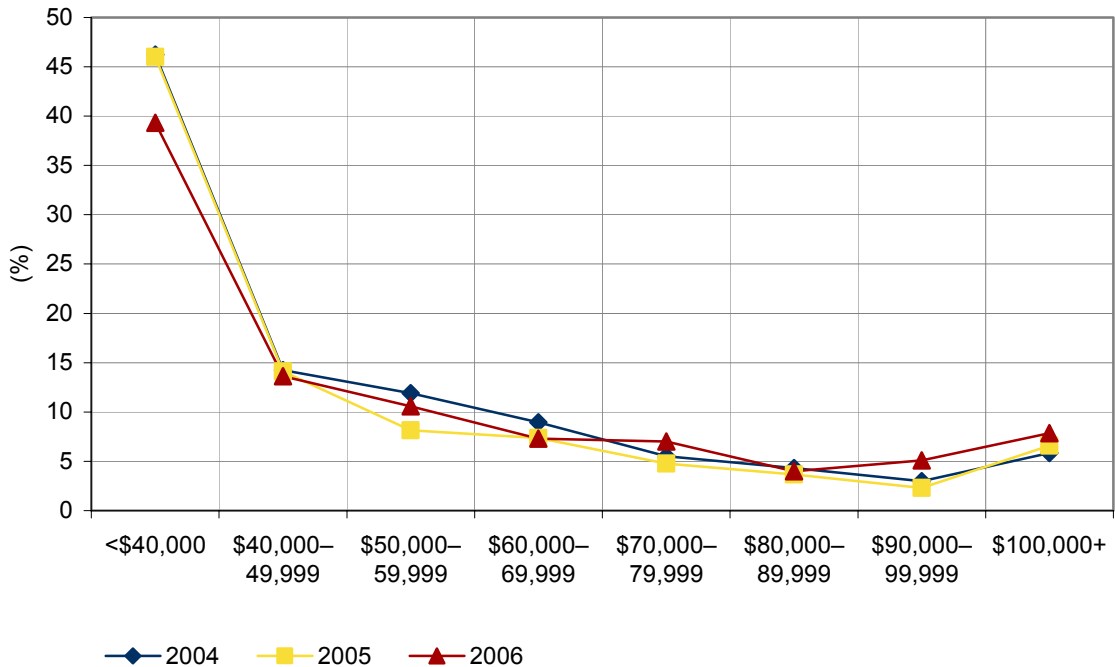
EMEA Salary Bands for Information Security Professionals, 2004–2006



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

**FIGURE 10**

Asia/Pacific Salary Bands for Information Security Professionals, 2004–2006



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

### **Certifications: Can They Sustain Their Value in a Maturing Market?**

Twenty years ago, no one had "practical" experience securing a network because it was a new area of IT and not a well-understood discipline. In lieu of experience, organizations and hiring managers relied upon certifications as a means of justifying hiring an employee. Attaining a security certification made an important statement to potential employers that an individual had the knowledge, skills, and abilities to defend an organization against possible breaches and build up defenses. This achievement placed a candidate ahead of the pack as additional metrics beyond certification were not available.

According to 33% of respondents this year involved in the hiring process for information security staff within their organizations, the importance of information security certifications as a hiring criterion remained high with 85% of hiring managers, but it has been declining slightly for managers since 2004 (see Figure 11). Looking at this year's results on a regional basis, we find that hiring managers in the Americas place slightly more importance on certifications than hiring managers in EMEA or

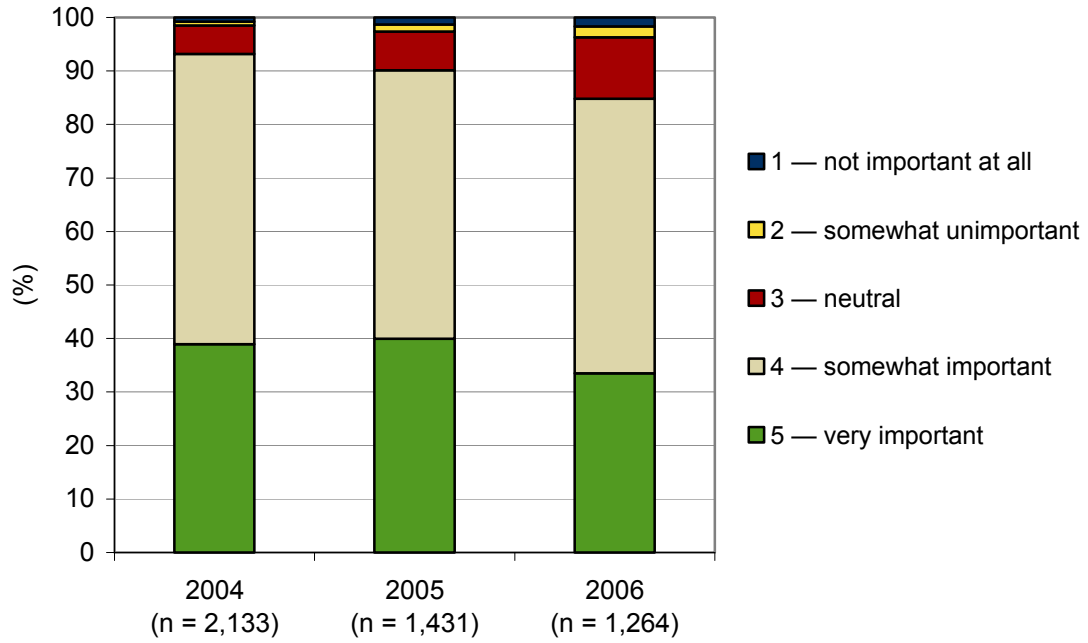
Asia/Pacific (see Figure 12). Domestically and internationally, more than 80% of respondents feel that certifications are still an important factor to consider in the candidate evaluation process. While certifications are one indication of a better candidate, they do not tell everything about the professional's total capabilities.

As managers have come to understand the limits of certification, hiring managers may be becoming less impressed with the book learning a candidate has than with the belief that the candidate can roll up his or her sleeves and take action. It is important to note, however, that all certifications are not created equal, and hiring managers should take note of the specific requirements of a certification or certification sponsor rather than simply the fact that there is a certification.

Complexity has been added to the hiring process over the years due to the sheer number and qualitative differences of certifications offered in the marketplace. The list of vendor-neutral and vendor-specific security certifications grows every year, making it difficult for employees, hiring managers, and their organizations to discern which certifications carry the greatest value for them. Six years ago, approximately 15 different security certifications were available in the marketplace. Today, the number has significantly grown to more than 40 vendor-neutral and more than 25 vendor-specific certifications. IDC believes the volume of certifications may cause a dilution effect in the marketplace, which will make it a challenge for all certifications to differentiate themselves in the future. Our concern is that certifications that are considered of high value today will become less significant to information security professionals and, more important, their employers in the future. The onus will shift onto the sponsors and providers of both vendor-neutral and vendor-specific security certifications to articulate their value and distinguish themselves from each other. Certification providers will need to highlight the rigors, qualifications, years of experience, and steps to attainment associated with their certifications. In the end, information security professionals will decide which certifications are of value to them.

**FIGURE 11**

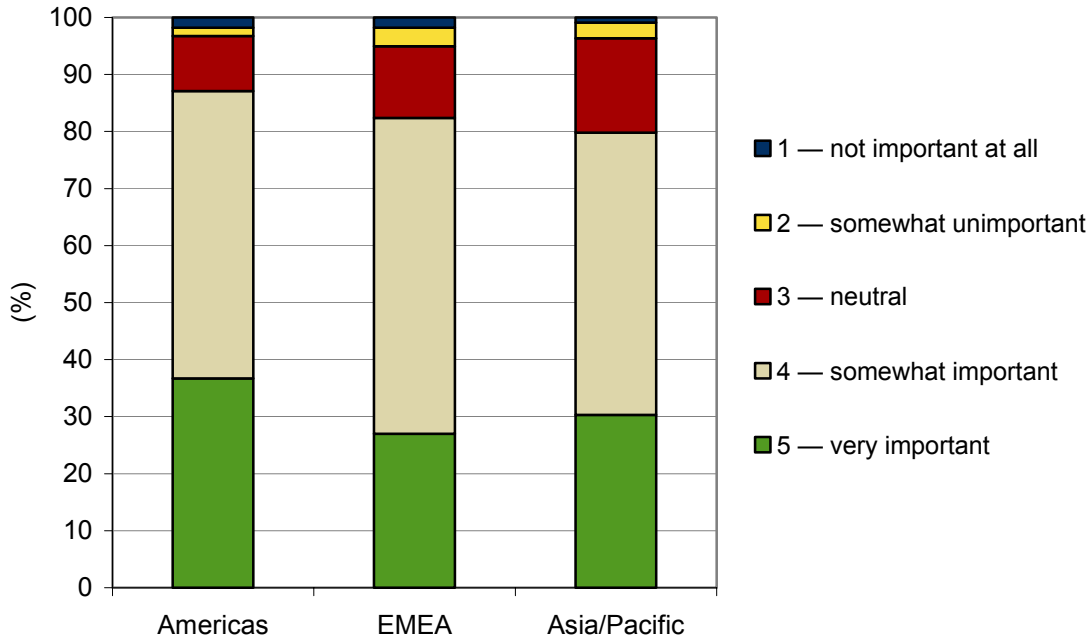
Importance of Information Security Certifications When Hiring Information Security Professionals



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

**FIGURE 12**

**Importance of Information Security Certifications When Hiring Information Security Professionals by Region**



n = 1,264

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

As they pertain to the candidate selection criteria of the organization, top reasons managers prefer hiring information security professionals with information security certifications are illustrated in Table 4. Employee competency and quality of work remain the major reasons; however, other reasons are surfacing. As the results of this year's study showed, more organizations are requiring their information security staff to hold certifications because of company policy and regulatory compliance. In the Americas, hiring managers are feeling the pressures of regulatory compliance and want to ensure their information security staffs are knowledgeable and skilled and carry the credentials to get them to compliance. One example in the U.S. is the Department of Defense (DoD) Directive 8570.1, which requires all DoD information assurance technicians and managers to be trained and certified to a DoD baseline requirement. Thirteen certifications have been identified and mandated by the Directive's enterprisewide certification program. Some hiring managers in EMEA and Asia/Pacific said their organizations are not requiring certifications of their staff. This is a slight increase over 2005 — not significant but something to watch.

**TABLE 4**

## Reasons Managers Prefer Hiring Information Security Professionals with Information Security Certifications by Region (% of Respondents)

	Americas			EMEA			Asia/Pacific		
	2004	2005	2006	2004	2005	2006	2004	2005	2006
Company policy	15.9	15.9	21.1	17.7	23.3	24.6	22.0	22.0	27.2
DoD Directive 8570.1			12.6			2.7			2.8
Employee competency	72.0	50.4	40.4	71.5	58.5	51.0	70.3	69.5	64.5
Legal/due diligence	24.6	15.2	15.1	15.4	14.8	12.2	17.6	13.9	16.2
Not required		37.1	34.7		26.1	27.5		13.5	15.1
Other (specify)	61.1	4.5	4.3	52.3	4.9	3.9	40.7	2.2	2.1
Quality of work	46.6	37.7	35.9	45.4	53.7	45.2	54.6	56.5	53.8
Regulatory requirements (governance)	13.7	17.5	20.8	8.5	15.7	14.7	12.1	19.0	18.7

n = 4181

## Notes:

- Multiple answers were allowed.
- In 2004, "Not required" was not a survey option. "Other" consisted of answers such as "personal preference" and "not required."
- In 2005, "Not required" was added as a survey option.
- In 2006, "DoD Directive 8570.1" was added as a survey option.

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

Relevant certification is a good reason to consider a candidate, but not the only reason to hire one. Hiring managers should also consider the candidate's experience with the software and hardware across the entire computing infrastructure; experience at responding to active attacks; experience with the security policies, protocols, and standards in place; and even experience mitigating risk. On balance, employers now have the ability to place greater importance on experience and work history in evaluating candidates because practical skills are now available in this maturing market. Both experience and certification are valuable. Employers should evaluate both and consider which is more important for a particular position.

### Information Security Certifications Remain Important

One critical value of certifications is that they establish a foundation from which conscientious professionals can build. Security threats are continually evolving, so security professionals must equally evolve their skills and utilize new tools and techniques to adapt and respond to the ever-changing threats. In some cases, a new certification might be the best approach to validating new skills, but regardless of the test professionals take, their success in the profession and their companies' ultimate protection will come from their ability to learn new defenses and to fully employ and leverage new security tools and techniques within the infrastructure and the entire organization.

Differentiation from other candidates and potential salary benefits have been other reasons individuals interested in information security obtain certifications. These additional benefits continue to be enjoyed by information security professionals, as demonstrated in the results throughout this study. In an effort to guarantee that they remain relevant, 57% of respondents said they would look for at least one more new certification to add to their toolkits in the 2006–2007 time frame. As they did in the 2005 study, information security professionals in Central and South America and CEMEA expressed stronger-than-average intent to attain more certifications.

In the future, security practitioners must 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 and service oriented architecture) and the changing nature of information security. Organizations are slowly and carefully moving toward a converged security environment in which physical and logical security operate over a single network. Technical knowledge will be important; however, knowing the business and utilizing business skills, such as communication, negotiation, and managing up and down, will become even more critical to an individual's career advancement and survival.

## **FUTURE OUTLOOK**

---

### **Moving Toward Risk Management**

In an effort to stay ahead of the curve, information security professionals identified additional training and education opportunities across a number of disciplines. First and foremost (see Table 5), the area of information security risk management has risen to the top in both the Americas and EMEA, while it is number 2 in Asia/Pacific. This has been the hot topic of 2006, and it will continue to be the hot topic in the foreseeable future as organizations struggle to gain control over their risk posture, develop a flexible framework to quickly adapt to new environmental factors, and provide visibility into their greatest risks. Other key topics for all three regions are business continuity and disaster recovery and forensics, which made the top 5 in 2005 as well. All of these topics are critical components of any organization's information security risk management program.

During 2005, ISO/IEC 17799 was the top priority for additional training in EMEA and Asia/Pacific. It remains one of the top 5 priorities this year, but it is seeing less emphasis in EMEA and did not even make the cut in Asia/Pacific. New on the radar screen of information security professionals across the Americas and Asia/Pacific is applications and system development security. The rise in attacks, particularly zero-day attacks, against the Web and other critical applications has stirred a movement to better understand security's role in application and system development life cycles. Interest is coming from both information security professionals and software developers alike.

As mentioned previously in the study, forensics is a hot issue as a result of large corporate scandals, identity theft, and data leakages. Some organizations attempt to clean up 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. For the most part, organizations would probably rather keep this in-house and deal with a situation internally, hence the need to train their staff on the techniques and evidence collection procedures of forensics.

**TABLE 5**

Top 5 Areas Identified for Additional Training by Region

Rank	Americas	EMEA	Asia/Pacific
1	Information security risk management	Information security risk management	Business continuity and disaster recovery planning
2	Forensics	Business continuity and disaster recovery planning	Information security risk management
3	Applications and system development security	ISO/IEC 17799 (Code of Practice for Information Security Management)	Security administration
4	Business continuity and disaster recovery planning	Forensics	Forensics
5	Security management practices	Security administration	Applications and system development security

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

### Sharing the Risk

Although the person responsible for maintaining security in an organization is the cornerstone of protection, security is ultimately everyone's duty. If any one individual fails to maintain and adhere to security policies, then all computing systems and the viability of the organization are at risk. As Figure 13 demonstrates, every C-level officer is accountable to some extent. IDC has observed the gradual shift in responsibility away from the CIO into other areas of senior management and the business. CEOs, boards of directors, chief information security officers, chief security officers, legal, heads of compliance, and chief risk officers are sharing accountability for the security and overall risk of the organization. If the regulatory environment continues on its current trajectory, these individuals may see more of the risk share in the near future.

This message has been a challenging one to impress upon management over the past two years. Information security professionals have remained positive about their ability to influence and have been instrumental in changing the mindset of executives and gaining their buy-in that security is an enterprisewide problem, not just an IT issue. During the past 12 months, 67% of security practitioners believe their efforts were effective in bringing change to their organizations. Anticipating the arrival of 2007, 73% of information security professionals remain optimistic that they will be able to influence management and the business stakeholders to drive security awareness and responsibility.

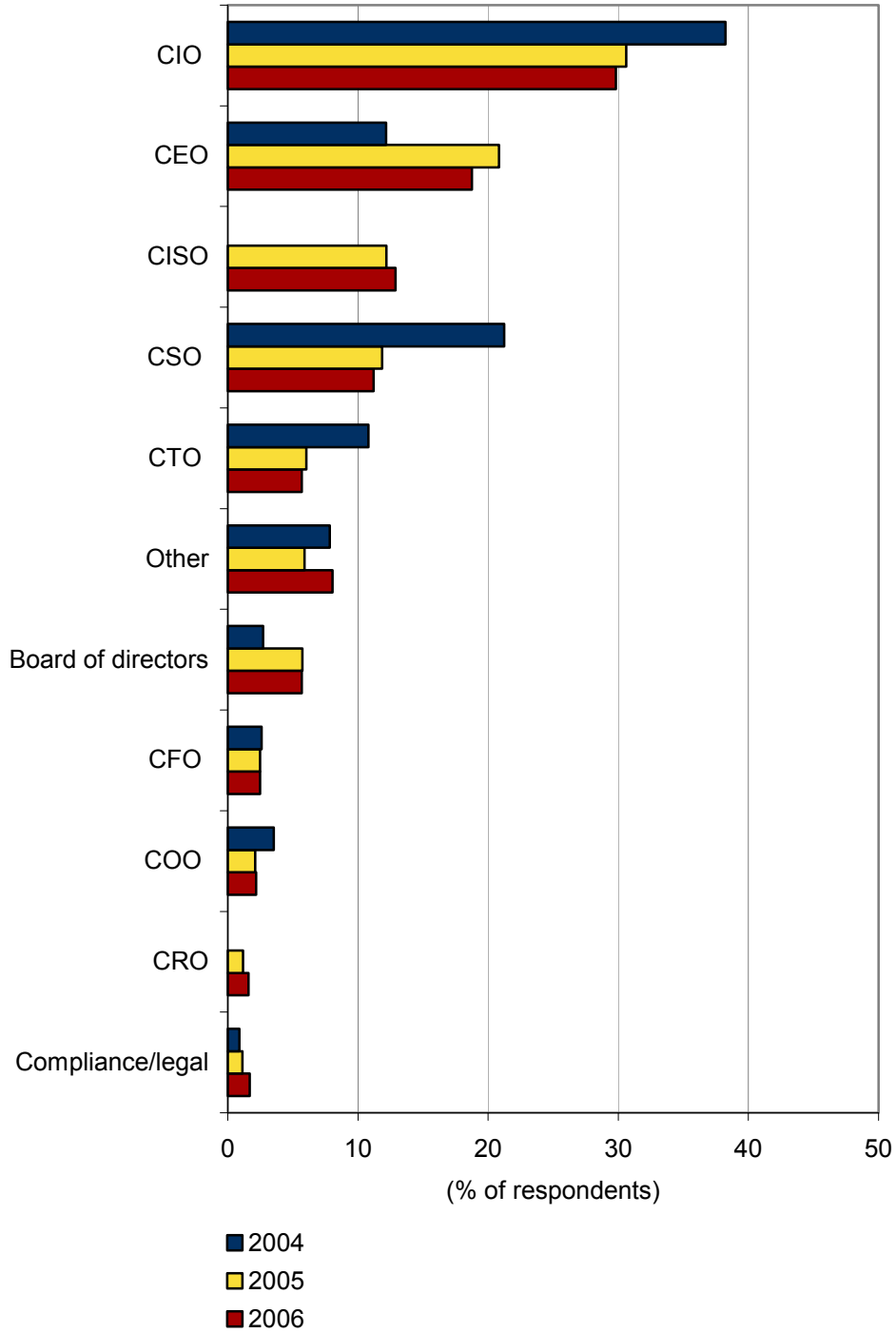
Much of information security professionals' time will be spent meeting with executives and management to discuss the significance of corporate security policies and why they should be implemented and, more important, enforced. According to the 2006 study, this is security practitioners' primary concern for effectively securing their organizations' infrastructures. The following list shows the factors (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

The top 3 highlight the need to focus more time and attention on policies, processes, and people — areas that have been overlooked in the past, in favor of deploying more technology to solve security problems. Information security professionals in each region unanimously acknowledged that technology is only an enabler, not the solution, to executing a sound security strategy and supporting a well-defined and well-articulated risk management program where everyone shares responsibility.

**FIGURE 13**

Individual with Ultimate Accountability for Organization's Information Security Functions, 2004–2006



n = 3,578

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

## CONCLUSION

Information security is a global, industry-agnostic, organizationwide problem that cannot be addressed with technology solutions alone. It requires the unconditional commitment of an organization at the financial, management, and operational levels to proactively secure and protect the organization's logical and physical assets. Security management will always require the proper balance between people, policies, processes, and technology to effectively mitigate the risks associated with today's digitally connected business environment.

IDC believes that the 4,016 information security professionals who shared their views and opinions in this study are taking this message to the masses and are acting as "change agents" within their organizations to ensure information security is recognized for its positive contributions to the business, as opposed to the sunk cost it has been perceived to be in past years. The message of people and processes being absolutely crucial to effective information security is finally starting to resonate with business leaders. As a result of the 2006 *G/SWS*, IDC advises information security professionals to consider the following conclusions:

- ☒ Senior executives remain ultimately accountable for security and risk management; however, others, such as the CRO and CISO, are shouldering the burden of accountability along with the CIO, CEO, and board of directors.
- ☒ People and processes are finally becoming recognized as the greater focal point for risk management efforts as technology is acknowledged to be an enabler for achieving organizational objectives, not the solution.
- ☒ Compliance is driving organizational behavior from changes in spending levels to shifts in accountability to requirements in new skill sets.
- ☒ Proliferation of information security certifications could have a dilution effect on their perceived value to hiring managers and professionals in the coming years if sponsors are not careful to articulate their differentiation.
- ☒ As emerging markets, Latin America, CEMEA, and Asia/Pacific offer attractive employment incentives and opportunities for information security professionals over the next five years.
- ☒ Security domains such as information risk management, business continuity, and forensics are topics where professionals are looking to increase their knowledge and sharpen their skills.

---

## Copyright Notice

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2006 IDC. Reproduction without written permission is completely forbidden.