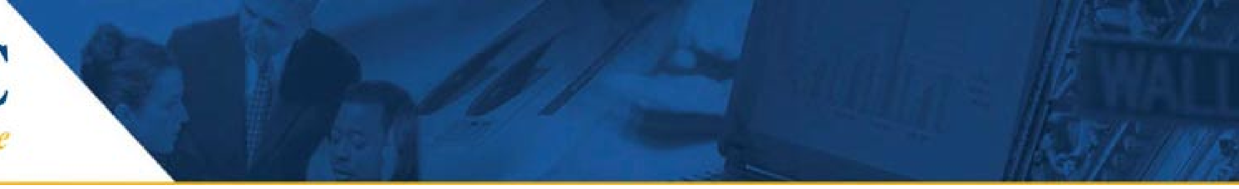


Analyze the Future

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

WHITE PAPER

2005 Global Information Security Workforce Study

Sponsored by: (ISC)^2

Allan Carey

December 2005

IDC OPINION

Information technology and information security have certainly undergone changes since IDC conducted its inaugural *Global Information Security Workforce Study (GISWS)* 12 months ago. Threats and attacks such as spam, phishing, malicious code, and spyware have been creeping up the corporate priority list and keeping information security professionals extremely busy patching, remediating, and sanitizing network environments under their management. In addition to their everyday responsibilities, security practitioners must continuously justify their spending and investments, demonstrate their value, and educate their management and customers about the operational risks facing their organizations. To perform all the requirements asked of them, security practitioners need a mixture of technical know-how, business savvy/acumen, and strong interpersonal skills. This study is designed to provide a snapshot of the security workforce today and a glimpse into the future of the information security profession. IDC remains positive on the outlook for this industry for the following reasons:

- Security is a constant for organizations; it is constantly dynamic, constantly required, and constantly pervasive.
- Shifts in attacks, tactics, and vectors require security professionals to fine-tune existing skills and learn new techniques.
- Dialogue between information security professionals and management has evolved from a technical discussion to a risk management comprehension.
- Lines between physical and logical security are blurring to provide seamless security and stronger accountability.

EXECUTIVE SUMMARY

On behalf of the International Information Systems Security Certification Consortium (ISC)^2, IDC was engaged for the second consecutive year to provide detailed insight into the important trends and opportunities emerging in the profession worldwide. The electronic survey was conducted via a Web-based portal, where 4,305 respondents from companies and public sector organizations around the globe offered their opinions about the information security profession in which they work full-time. 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 2005 is estimated to be 1.4 million, a 9% increase over 2004.

- Security's influence on line-of-business (LOB) owners, executives, and board members continues to increase during 2005. Seventy-three percent (73%) of practitioners believe this level of influence will persist into the future as well.

- Organizations spend on average more than 40% of their IT security budgets on personnel, including salaries and benefits, and on internal and external education and training.

- The number of individuals reporting achievement of a master's degree or its equivalent first stage of tertiary education was up in 2005. For example, 42% of professionals in Europe, Middle East, and Africa (EMEA), compared with 32% last year, reached this level of education.

- The Asia/Pacific (AP) region represents a less mature, faster-growing population of information professionals than other regions, with an average of 6.6 years of security-related experience.

- Employers and hiring managers continue to place emphasis on security certifications as a differentiator in the hiring process. The main reasons provided were employee competency and quality of work.

- More than 60% of information security professionals stated that they intend to acquire at least one more certification in the next 12 months.

- In terms of future demand, security professionals are asking for education in the areas of business continuity planning, forensics, and information risk management.

Continuing education plays an important role in enabling individuals to prepare and achieve differing levels of certification, from basic, entry-level to more advanced specialization. On average, 86% of security professionals said that security certifications are important to their career advancement. Certifications are not only important from a career standpoint, but further training enables professionals to stay on top of the most current trends, identify how trends will impact risk to their organizations, and determine best solutions/practices for mitigating risk in the overall context of their organizations' risk management strategies. The result is that practitioners will be better positioned to have a positive impact on the business and be rewarded by progressing up the organizational hierarchy.

Information security professionals are trying to differentiate their capabilities in a marketplace that remains competitive and complex, requires expertise, and demands results. In order to further their careers, security professionals must be perceptive of the trends and forces influencing the information security workforce.

METHODOLOGY

The 2005 *Global Information Security Workforce Study (GISWS)* was conducted during the summer of 2005 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 second 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. 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 4,305 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

Respondent Profile

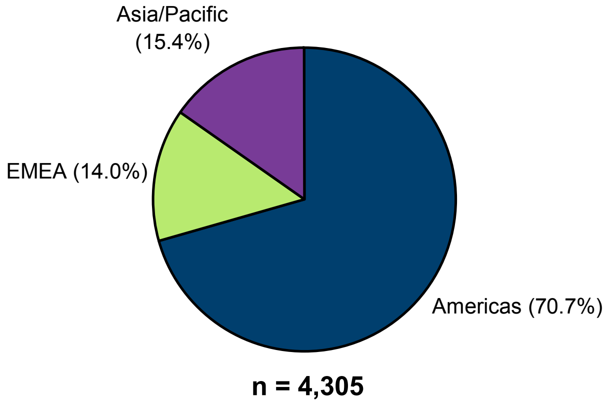
The respondents to the survey represent organizations of various sizes, different vertical industries, and varying core competencies and skill sets from 81 countries around the world (see Figure 1). From Argentina to Singapore, regional respondents in the Americas (North, Central, and South); EMEA; and AP play a vital role in their organizations' information security activities. Each respondent has a role in purchasing, managing, or maintaining a multitude of IT security technologies, services, and/or personnel. Any individuals that are solely responsible for physical security were not included as part of this study.

In terms of functions, most respondents were at the security engineer level or higher within their organizations. More than two-fifths of the respondents were security consultants (i.e., individuals speaking to and advising organizations on their security strategies and challenges). Almost 10% consisted of executive management, with the remainder consisting of various security titles (see Figure 2).

With titles such as chief information officer (CIO), chief security officer (CSO), and chief information security officer (CISO), the respondents were qualified as having both knowledge of and responsibility for security initiatives within their organizations.

FIGURE 1

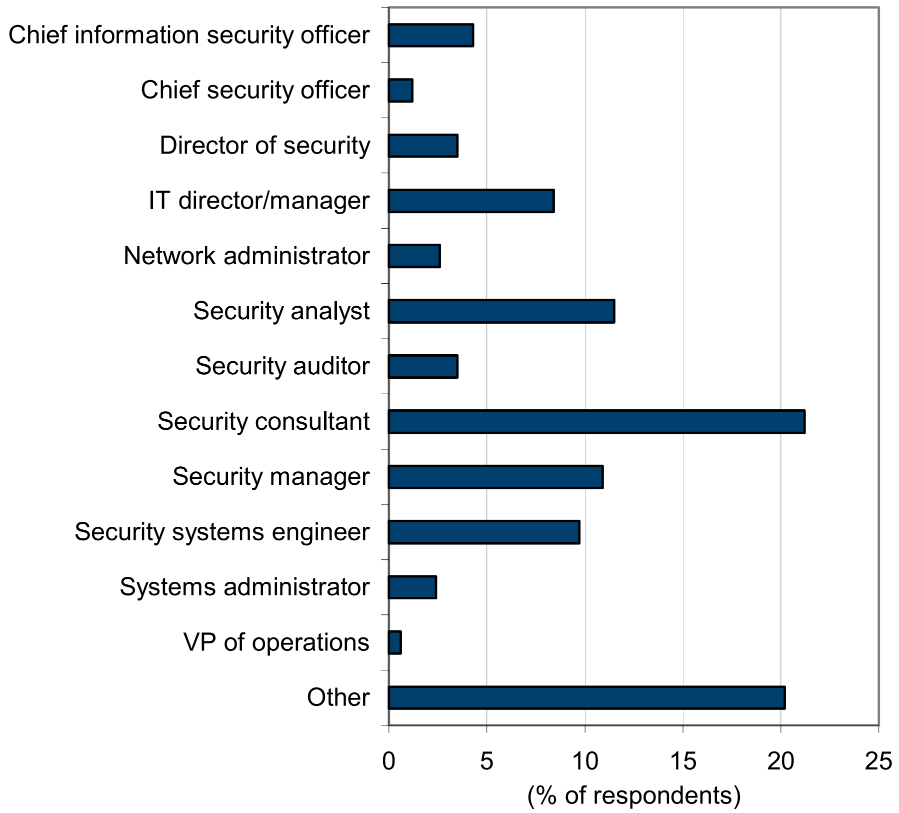
Respondents by Geographic Region



Source: IDC's *Global Information Security Workforce Study*, 2005

FIGURE 2

Respondents by Job Title or Function



n = 4,303

Note: The "other" category includes titles such as information assurance officer, information security officer, chief risk officer, and security architect.

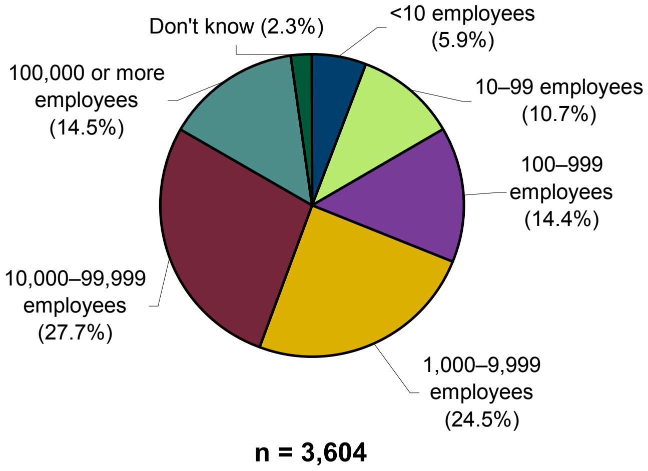
Source: IDC's *Global Information Security Workforce Study*, 2005

Organization Profile

Organizations of many sizes participated in the survey. For segmentation purposes, organizations were split into multiple categories (see Figure 3). More than 66% of responding organizations had more than 1,000 employees, while 16.5% had fewer than 100 employees. The remainder would be considered midmarket or medium-sized organizations.

FIGURE 3

Respondents by Company Size

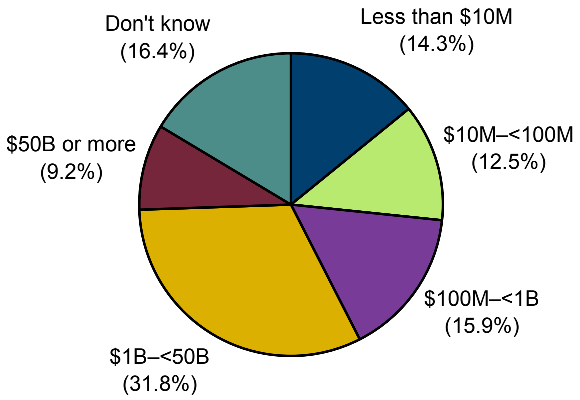


Source: IDC's *Global Information Security Workforce Study*, 2005

In addition to being asked about the size of their organizations, respondents were asked about their organizations' annual revenue. Forty-one percent (41%) of the responding organizations generated more than $1 billion in annual revenue. Moreover, 27% generated less than $100 million in annual revenue (see Figure 4).

FIGURE 4

Respondents by Company Revenue



n = 3,498

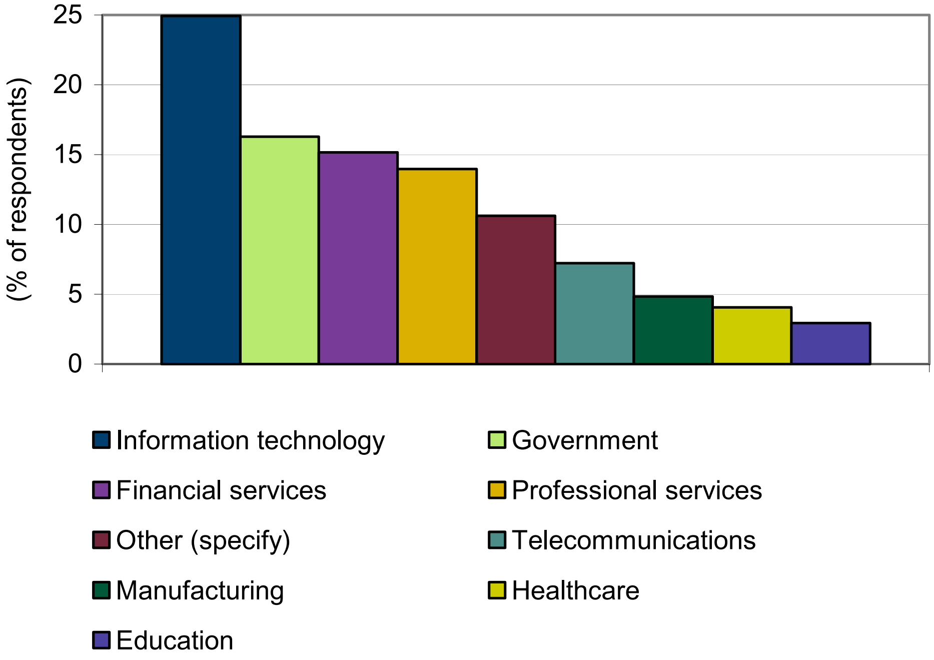
Source: IDC's *Global Information Security Workforce Study*, 2005

Industry

Organizations from both the public and private sectors were represented. Banking, healthcare, government, manufacturing, and utilities were just a few of the responding industries facing increasing security requirements and challenges (see Figure 5). The IT industry, consisting primarily of hardware and software technology vendors, was the largest segment; followed by the government sector.

FIGURE 5

Respondents by Vertical Industry



n = 4,305

Note: The "other" category includes industries such as entertainment, pharmaceuticals, biotechnology, and hospitality.

Source: IDC's *Global Information Security Workforce Study*, 2005

The sample in this study is not designed to reflect the universe of all public and private organizations, and the results should not be projected across the entire population at large. Rather, the data points are meant to be interpreted as leading market indicators and reflect the opinions of the 4,305 individuals surveyed for this IDC study.

SITUATION OVERVIEW

Introduction

Information security has become a critical component of enterprise and government risk management programs on multiple fronts. Business leaders worldwide are taking a serious look at the risks and opportunities presented when data resides at the center of almost every core business activity in which they are engaged. Additionally, they are acting more proactively because market forces are placing more accountability for the risk — and protection — of the organization upon them.

Consequently, security is no longer viewed merely as an administrative detail on the overhead budget or a technical issue easily addressed with the latest off-the-shelf technology product. Security has risen to the top of the corporate agenda as a strategic business process that affects what organizations value most: their mission, ability to execute, and accountability to stakeholders. Complex security solutions, regulatory requirements, and encroaching threat advances are driving organizations to develop, employ, and enforce enterprisewide security strategies and risk management programs. Security teams must now perform an ever-growing list of activities such as threat mitigation, compliance auditing, and proactive security management and monitoring.

Viruses and worms continue to be the most serious threats facing corporations today. According to IDC's 2004 *Enterprise Security Survey* of more than 600 firms across North America, 31% of respondents identified viruses, trojans, and malicious code (not including distributed denial of service attacks) as the single greatest threat, and an additional 12% identified unintentional employee error as the greatest threat. An interesting finding in the survey was that spyware ranked fourth on the list of single greatest threats in 2004. This result clearly shows that spyware is becoming more prevalent on the priority list of corporate information security concerns, which will require new technology solutions and greater staff skills to gain control of the problem.

Everyone — from executives to LOB leaders to IT departments — is being asked to contribute scarce resources and to support information security activities through a variety of means. At the same time, these groups are struggling with the rising costs of dealing with old and new security issues as well as the ever-present viral unknown. To combat the rising tide of threats, many enterprises are seeking solutions in response to their increasing popularity and effectiveness. As a result, information security spending remains a top priority in many organizations. The total worldwide IT security market achieved a level of $27.2 billion in 2004, representing 19% growth over 2003 (see *Worldwide IT Security Software, Hardware, and Services 2004–2008 Forecast: The Big Picture*, IDC #32557, December 2004).

Security education and training is a subsegment of the total IT security market. IDC expects spending on information security training and education in the United States alone to reach approximately $1.6 billion by 2009, representing 16.4% year-over-year growth (see *Worldwide and U.S. Security Services 2005–2009 Forecast*, IDC #33106, March 2005). Within the segment, training and education is provided for security awareness, vendor-neutral and vendor-specific courses and certifications, and other security-related curricula.

Time and time again, IDC observes the need for more 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. According to IDC's *Enterprise Security Survey* conducted earlier this year, 37% of individuals stated that if given a larger security budget, they would initially increase the size of their IT staff dedicated to enterprise security and better train employees to avert human error. Anecdotally, many providers of security services are struggling to find appropriate candidates for the vacancies within their security workforces. Consequently, opportunity awaits those individuals looking to enter into an information security career path.

Factoring in a number of market dynamics, including organization size, IT budget, and vertical industry, IDC estimates the number of information security professionals worldwide in 2005 to be 1.4 million, a 9% increase over 2004. This figure is expected to increase to more than 1.9 million by 2009, displaying a compound annual growth rate (CAGR) of 8.5% from 2004 to 2009 (see Table 1). The market outlook remains positive for individuals seeking to diversify their skills and differentiate themselves in the workforce. IDC's projections are not as aggressive as previously stated in the 2004 study, which illustrated a 13.7% CAGR during the 2003–2008 time period. 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 2005–2009 based on reported and observed trends and events in 2004 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 Professional Forecast by Region, 2004–2009

							2004–2005	2004–2009
	2004	2005	2006	2007	2008	2009	Growth (%)	CAGR (%)
Americas	558,652	606,268	647,577	693,218	735,709	787,292	8.5	7.1
EMEA	320,005	348,162	379,142	407,917	437,463	467,386	8.8	7.9
AP	414,802	459,593	509,644	568,760	630,045	689,345	10.8	10.7
Total	1,293,459	1,414,023	1,536,364	1,669,894	1,803,217	1,944,022	9.3	8.5

Key Assumptions:

- Growth in the number of IT employees globally will be 4.8% during the forecast period.
- The Americas region, particularly the United States, is more advanced in security adoption than other parts of the world.
- Security staffing requirements vary depending on company size, business model, industry, and IT budget.
- Interest in gaining IT 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 IT staff dedicated to security activities will always be required.
- Asia/Pacific remains a growth area for technology and outsourcing and will attract individuals to meet the demand.

Note:

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, 2005

In the 2004 *GISWS*, government regulations, emerging technologies, and an escalating threat landscape were mentioned as contributing factors for growth in the demand for information security professionals. These issues remain present in 2005; however, organizations have been cautious to allocate more staff resources and increase headcount to solve their problems. Stringent financial controls and business case justification are increasingly being utilized to evaluate the need for additional information security professionals. However, moving forward, growth in the market for information security professionals will be influenced by a number of factors:

- **Budgets.** As organizations change their view of information security from a discretionary expenditure to a requirement, improved financial conditions will allow dollars to become available for investments and staffing.
- **Prioritization.** Security is becoming a top-level concern for organizations outside North America, causing security positions to be created and filled.
- **Services.** Organizations are leveraging security service providers to augment internal security staff or fill the void in skill sets, thereby alleviating some of the security burden.

State of the Market

Security Trends and Challenges

Last year, IDC mentioned that security breaches were costly, authors of malicious code had an impact on IT organizations, and security required a more proactive approach. These factors remained consistent throughout 2005, with a few exceptions. Malicious code writers and spammers have become more focused in their attacks, and their motivations are much more financially driven than in previous years. Hence, breaches and vulnerabilities are more costly to remediate and recover. In addition, the following trends have influenced this year's security direction:

- **Security is becoming operationalized.** Movement is away from reactive security, and a more proactive risk management approach is taking hold in large organizations.
- **Government compliance requires due diligence and a longer-term strategy.** Regulations are forcing organizations to evaluate and modify their business processes and operations with security in mind.
- **Complexity persists as a security factor.** The growing number of systems, networks, applications, and users creates an enormous management challenge.

All of the above factors are contributing to the movement within organizations to align their business and security strategies with the goal of establishing a comprehensive information risk management program. As a result, information security practitioners and their colleagues have spent a disproportionate amount of time and resources researching and implementing new technologies, demonstrating regulatory compliance, and addressing internal political issues. They perform all these activities while maintaining their daily responsibilities. The bottom line is that information security groups are not a cost center but rather a business enabler, and therefore, they must compete with other business groups for scarce resources such as staff and budget.

Information security practitioners and their colleagues have spent a disproportionate amount of time and resources researching and implementing new technologies, demonstrating regulatory compliance, and addressing internal political issues.

Research conducted by security professionals has resulted in recommendations and investments in some security solution areas. Table 2 highlights the top 5 security deployment areas for each region. Some common areas where organizations are investing their security dollars are wireless security, identity and access management, business continuity, and security event or information management.

TABLE 2

Top 5 Security Technology Solutions Being Deployed by Region

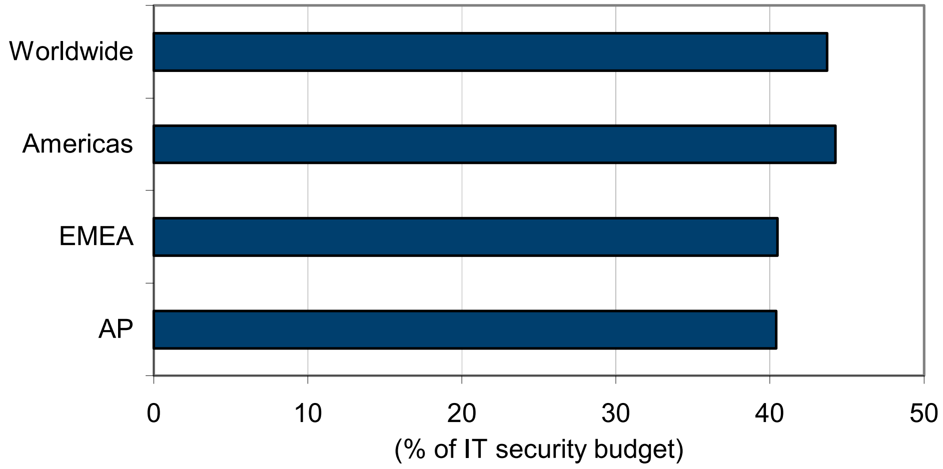
Americas	EMEA	AP
• Wireless security solutions	• Identity and access management	• Wireless security solutions
• Identity and access management	• Security event or information management	• Identity and access management
• Intrusion prevention systems	• Business continuity and disaster recovery solutions	• Business continuity and disaster recovery solutions
• Security event or information management	• Risk management solutions	• Forensics
• Business continuity and disaster recovery solutions	• Wireless security solutions	• Security event or information management

Source: IDC's *Global Information Security Workforce Study*, 2005

Currently, organizations spend on average more than 40% of their information security budgets on personnel as well as education and training. This number includes any expenditure to attract, hire, and retain the necessary security professionals required to achieve an organization's security and business objectives, as well as any internal and external security-related training delivered to employees. Figure 6 provides some insight into how organizations in different regions fund their security staffing requirements. The spending level in the Americas region, which is heavily influenced by the United States, is slightly higher than the worldwide average due to the high cost of living. EMEA and AP spend slightly less than their counterparts in the United States. Overall, organizations in Central America and South America; Central Europe, Middle East, and Africa; and AP spend significantly less on their overall IT security budgets than their counterparts in other regions of the world.

FIGURE 6

Percentage of IT Security Budget for Personnel and Training



n = 1,602

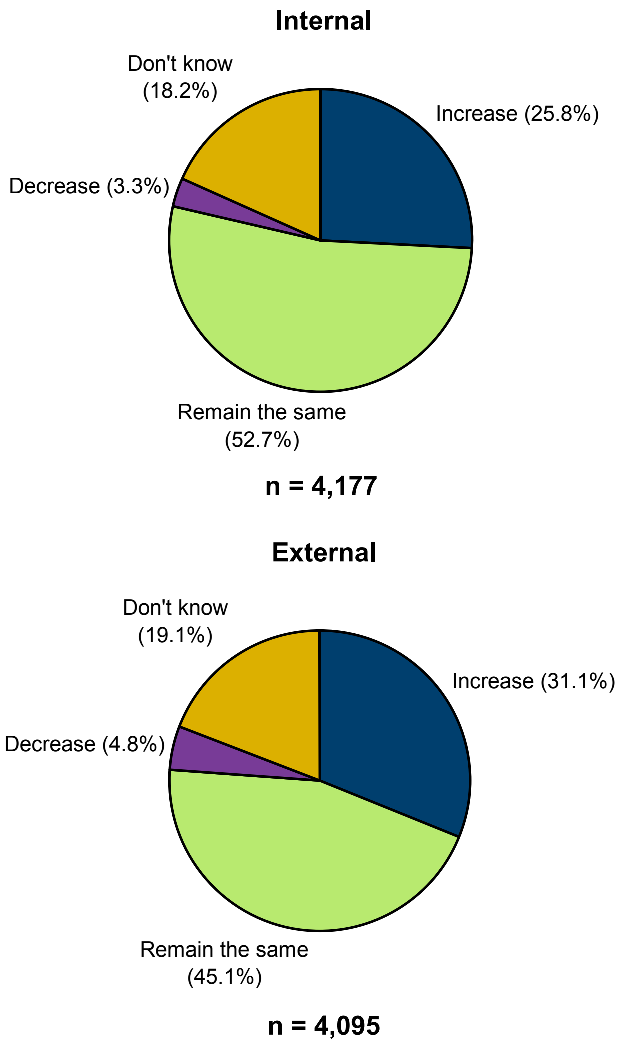
Note: The percentage represents the average across company size within the region.

Source: IDC's *Global Information Security Workforce Study*, 2005

The level of education and training provided by both internal and external sources is anticipated by respondents to increase by 22% in the coming year. As Figure 7 shows, a majority of respondents believe that training levels will remain the same as the year progresses. Professionals in AP (approximately 40%) were more optimistic about receiving increased levels of security training and education, 22% more from internal and 25% more from external sources.

FIGURE 7

Expected Change in Amount of Information Security–Related Training in Next 12 Months



Notes:

Internal refers to training received from the organization.

External refers to training received from an outside third-party provider.

Source: IDC's *Global Information Security Workforce Study*, 2005

Information Security Professional Profile

In 2005, like last year, the majority of respondents (90.5% in 2005 versus 88.9% in 2004) were male. EMEA and AP had higher male participation, 96% and 94%, respectively. The highest female response (12%) came from the United States. Men continue to dominate the information security workforce; however, more international programs are needed to foster career development and encourage female participation in the information security profession.

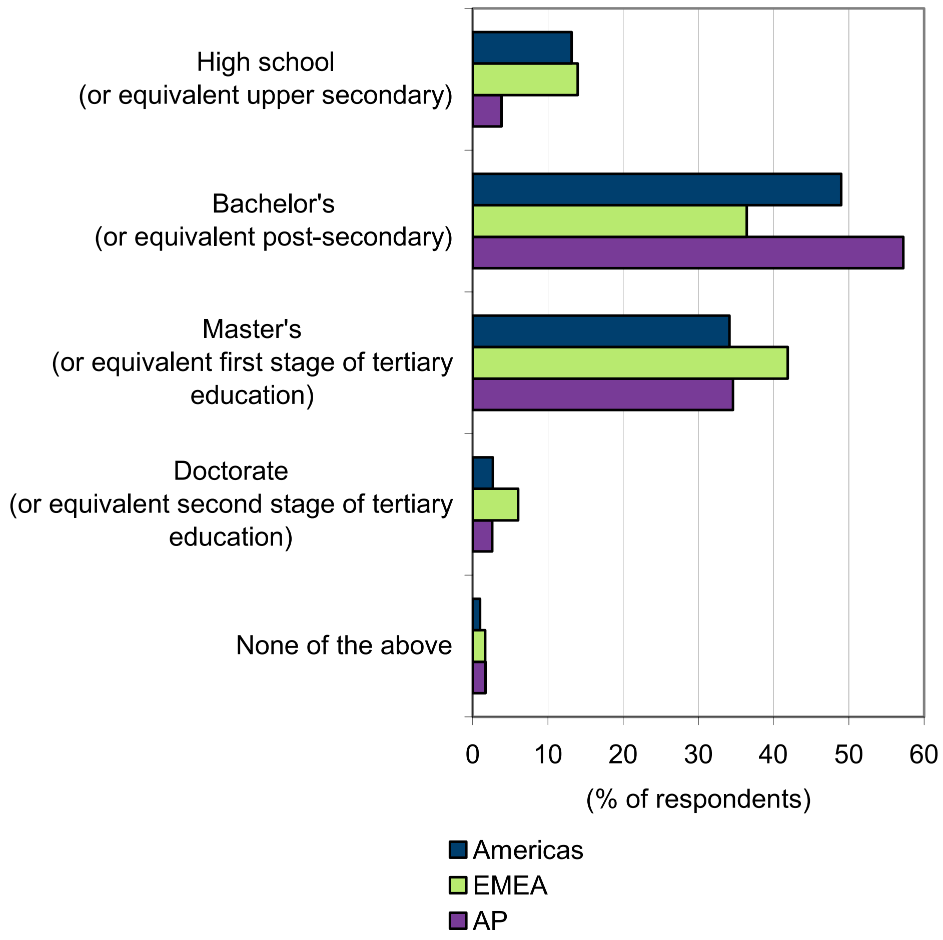
From an education perspective, the men and women in information security are highly educated, with many achieving advanced degrees (see Figure 8). At a minimum, the majority of those surveyed had a bachelor's degree or its equivalent post-secondary based on the International Standard Classification of Education (ISCED). A noticeable change from 2004 is that more individuals reported attaining a master's degree or its equivalent first stage of tertiary education. Forty-two percent (42%) of professionals in EMEA reached this level of education in 2005, compared with 32% last year. Within the Americas, the number of individuals completing a master's program increased significantly from 28% to 34%. Included this year, doctorate-level (or equivalent second stage of tertiary education) status was reported by 11% of information security professionals worldwide.

A noticeable change from 2004 is that more individuals reported attaining a master's degree or its equivalent first stage of tertiary education. Forty-two percent (42%) of professionals in EMEA, compared with 32% last year, reached this level of education. Within the Americas, the number of individuals completing a master's program increased significantly from 28% to 34%.

In addition to their educational achievements, security professionals have gained another valuable — and challenging — year of experience. Many lessons have been learned, such as achieving BS7799/ISO 17799 certification, locking down PCs, and controlling spam, and best practices are being utilized in conjunction with standards to drive information security strategies and establish frameworks to measure security progress. In 2004, the average security professional across each region had been in the industry for 8 years (Americas), 6 years (EMEA), and 5 years (AP). This year, security professionals in the Americas averaged 10.6 years of experience, while security professionals in EMEA and AP averaged 8.6 years and 6.6 years, respectively.

FIGURE 8

Highest Level of Education Obtained by Information Security Professionals by Region



n = 4,294

Source: IDC's *Global Information Security Workforce Study*, 2005

Table 3 provides further segmentation of the security workforce by looking at the percentage of professionals with less than five years, five to less than 10 years, and 10 years or more of experience in information security. Within AP, less than a quarter of information security professionals have yet to be in the profession for more than five years, illustrating the growth potential and appetite for security skills in the region. The security workforce in the Americas appears to be the most mature and experienced globally. For all of EMEA, there is a bifurcation between Western Europe and Central Europe, Middle East, and Africa. The percentage of individuals with less than five years of IT security experience in Central Europe, Middle East, and Africa is double that of Western Europe (20% versus 10%). In addition, there are 30% more security professionals with more than 10 years of experience in Western Europe than in Central Europe, Middle East, and Africa. The results suggest that the security profession in Central Europe, Middle East, and Africa is not as mature as Western Europe's.

TABLE 3

Years of Information Security Experience by Region (% of Respondents)

	Worldwide	Americas	EMEA	AP
Less than 5 years	12.2	9.6	12.5	23.6
5 to less than 10 years	47.7	43.8	53.6	59.1
10 years or more	40.0	46.6	33.9	17.4

Source: IDC's *Global Information Security Workforce Study*, 2005

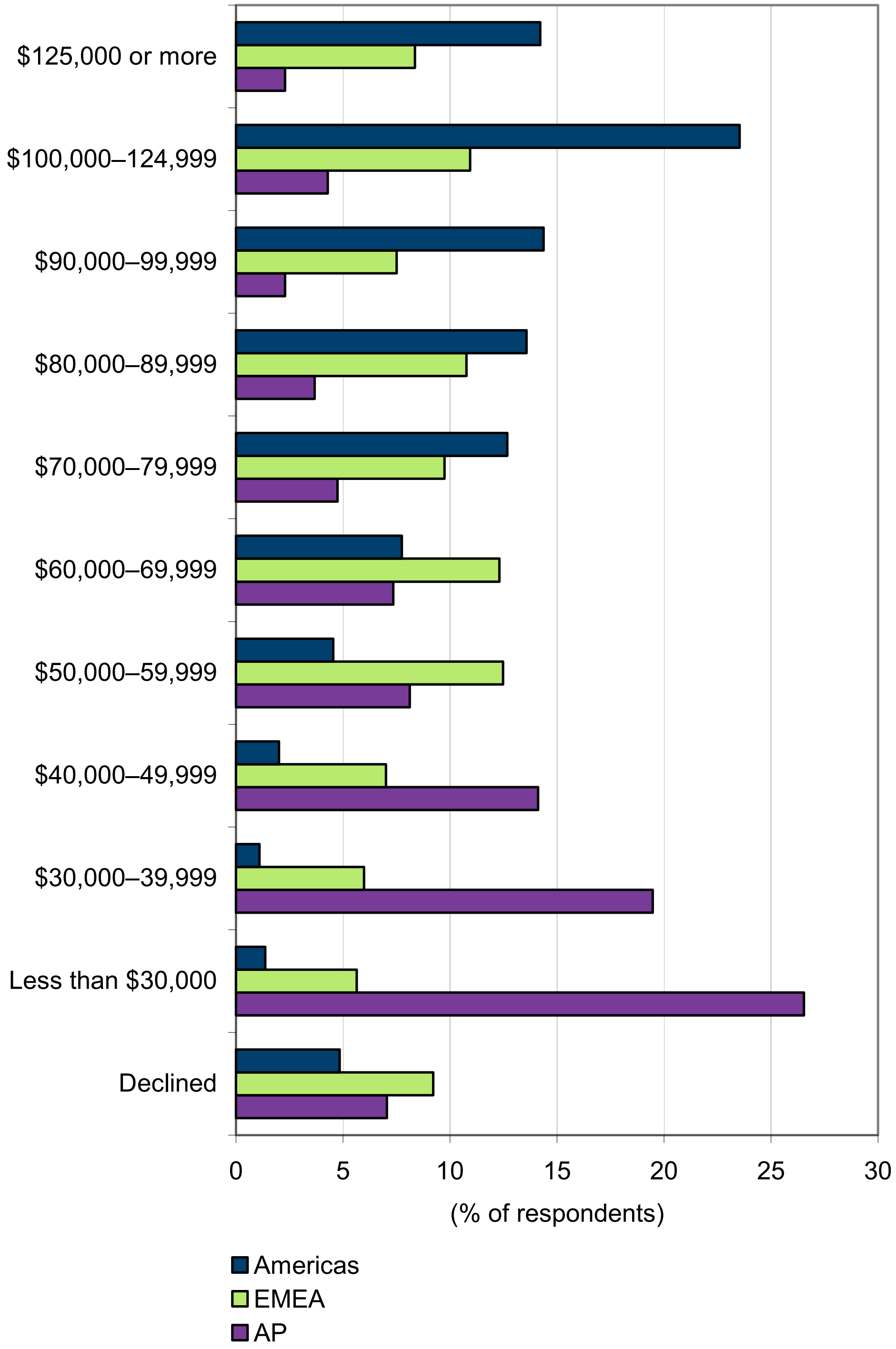
Typically, salary reflects or takes into consideration education and years of experience. Are information security professionals better paid this year than they were in 2004? It depends on the region in which they live and work. Figure 9 provides a breakdown of salary bands by geographic region. General trends indicate that the majority of security professionals from the Americas enjoy higher salaries than their peers in other regions, given that more than 46% of the workforce has over 10 years of experience. The percentage of individuals in the Americas earning more than US$125,000 per year increased by 4% this year and fell slightly (2%) for individuals in EMEA, while AP was relatively unchanged. A notable trend occurred in the percentage of information security professionals earning less than US$30,000 in AP. In 2004, approximately 24% of respondents fell into this category, compared with more than 26.5% in 2005. Labor arbitrage continues to be a strong economic factor in the AP region for those organizations looking to drive out operational staffing costs. Conversely, this increase suggests the number of young information security professionals accepting entry-level positions is on the rise to meet the demands of organizations to improve their security posture.

Who are security professionals reporting to within their organizations? According to the study results, almost a third (on average 32%) are reporting to the IT department, which is on par with last year's findings. Second, 20% have direct reporting lines to the security department or information assurance group. Third, 18% of all responding information security professionals report directly to senior-level executives. In 2004, the descending order of departments with the most security professional reports was IT, executive management, and security. As a result, in 2005, the security department has risen above executive management in the ranking. IDC attributes this year's shift in ranking to a greater number of individuals employed by the security group, the convergence of information security capabilities under one management, or possibly the consolidation of information security staff stemming from merger and acquisition activity. Nonetheless, the percentage of security professionals directly reporting to executives remained consistent with that of the previous year and has therefore continued to influence organizational strategies and decisions from a security and risk perspective.

Across all three regions, the results were fairly consistent. Furthermore, 6% report to the board of directors and 3% to the risk management group. Some of the reporting areas mentioned in the "other" segment were audit or internal audit, engineering, legal/general counsel, and professional services.

FIGURE 9

Salary Bands for Information Security Professionals by Region



n = 4,268

Source: IDC's *Global Information Security Workforce Study*, 2005

Why Get Certified?

Technology is changing at an incredible pace, and practitioners of technology must keep their skills fresh and sharp, particularly employees who are evaluating, deploying, and managing security solutions. The rapid pace of innovation within emerging security technologies is creating confusion as to how they integrate into the overall security architecture and framework, the specific problems they solve, and the business impact to the risk profile of the organization. However, the security solutions cannot deliver on their value propositions and expected benefits if the humans configuring and managing the solutions are doing so improperly. For this reason, security education and certification have become paramount to the success of any comprehensive and critical information security strategy.

From an employer's point of view, candidates or employees add value if they have an advanced education, years of experience, excellent interpersonal skills, and credentials. Credentials illustrate an individual's foundational knowledge of a certain topic or area. They can consist of both vendor-neutral and vendor-specific education, including certificates and certifications.

Employee Perspective

Employees have a vested interest in attaining continuing education credits and certifications as part of their career development paths. Some employee benefits to gaining certification are as follows:

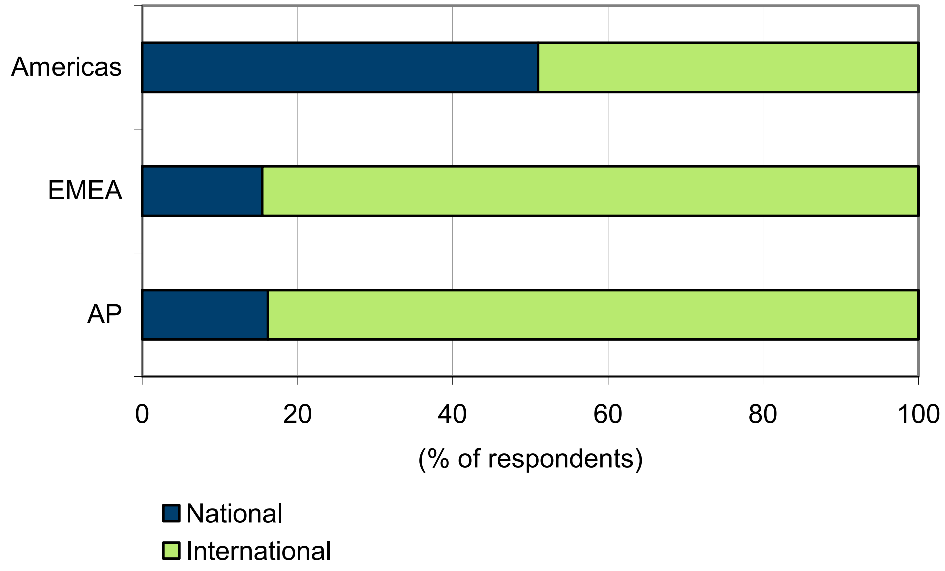
- Security certifications afford employees the opportunity to differentiate themselves within an increasingly competitive marketplace.
- Candidates can illustrate a base level of knowledge in security best practices, policies, and technologies. They can also strive for advanced specialization within the security field.
- Higher salaries may be negotiated based on certification type and market value.

When asked about the value of a certification with national recognition (i.e., in-country or regional standing) versus international status, employees from the EMEA and AP regions placed a significantly higher value on internationally recognized credentials than their colleagues in the Americas (see Figure 10). Within the Americas, respondents from the United States are heavily influencing the sentiment in the region, whereas information security professionals from Canada and Latin America (more than 80% in favor of international status) are in alignment with EMEA and AP.

IDC asked respondents the same question about the importance of national/international credential recognition to their employers. As shown in Figure 11, respondents believed that their employers would place the same amount of emphasis on international recognition as they do. Again, EMEA and AP placed more emphasis on international than national (75/25% split). Meanwhile, U.S. security professionals believed that their employers would be more inclined to value nationally recognized certifications (64%) over international certifications (36%). This response is a stark contrast from that of the rest of the world, where information security professionals outside the United States had almost the opposite view of how employers would value internationally recognized certifications.

FIGURE 10

Value of Credential Recognition to Employee

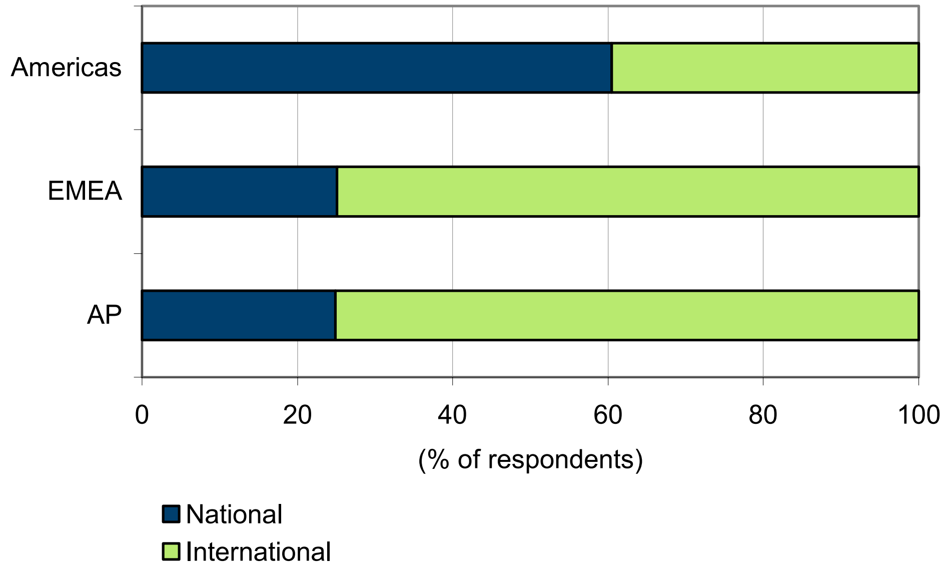


n = 4,213

Source: IDC's *Global Information Security Workforce Study*, 2005

FIGURE 11

Value of Credential Recognition to Employer



n = 4,115

Source: IDC's *Global Information Security Workforce Study*, 2005

Of the 4,305 respondents, 66% thought it is important for information security certifications to be accredited under the ISO/IEC 17024 standard. Professionals were unchanged in their view from a year ago and still believe ISO/IEC 17024 is an important characteristic for them to be able to transfer their skills from region to region or country to country. IDC further believes that the standardization of certifications will promote cross-pollenization and best-practices sharing of the information security workforce.

Employer Viewpoint

During the 2004 survey, IDC inquired about the importance of certifications to those who hire information security professionals within their workplaces. Forty-two percent (42%) of respondents actively involved in making hiring decisions related to their organizations' internal IT security staff stated security certifications are either somewhat important or very important when hiring decisions are being made. In fact, an average of 93% of these global security managers believed this to be true.

In 2005, 33% of the 4,305 respondents worldwide are responsible for making hiring decisions. Ninety percent (90%) of the individuals involved in the hiring process view certifications as either somewhat important or very important in their decision-making process (see Figure 12). Their opinions of certification importance did not differ significantly based on their location in the world. In fact, hiring managers in the United States place a slightly higher level of importance on certifications than hiring managers in other regions, as illustrated in Figure 13. In 2005, as in 2004, the minority of security professionals involved in the hiring process perceive certifications as unimportant.

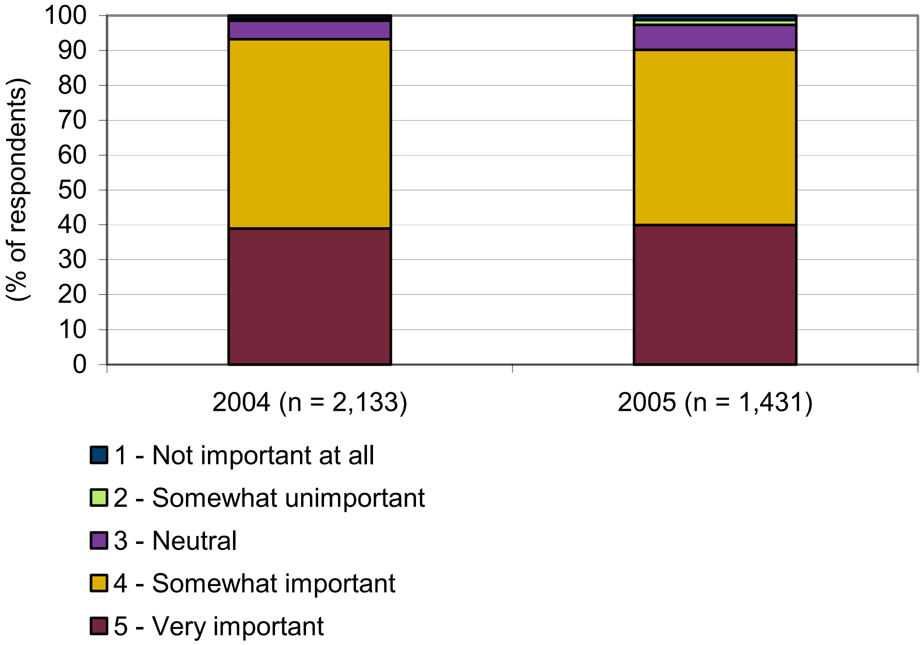
The overall top 3 responses regarding the importance of certifications this year are employee competency, quality of work, and staff is not required to have security certifications. These responses are in alignment with the reasons given in 2004. Last year, the top 3 reasons were employee competency, quality of work, and personal preference. Surprisingly, in the United States, a third of professionals responsible for hiring new security staff stated that security certifications were not required, which was the largest response of any region. Even though organizations did not require certifications, hiring managers did mention other reasons, such as personal preference and employee competency, as factors in the decision-making process.

Organizations believe employee competency is the major driver for certification considerations. By requiring certifications, organizations eliminate much of the unknown factor from the hiring equation and achieve some degree of comfort or a guarantee as to an individual's competency/knowledge level. Certification can be critical in terms of mitigating any associated risk or legal liability that may arise from an employee's actions. Regional differences are highlighted in Figure 14.

Findings of this study, and IDC's ongoing interviews and discussions with information security professionals at a wide variety of organizations worldwide, reveal that training classes are heavily attended and employers are beginning to require certification. For these reasons and as a result of the findings of the *GISWS*, IDC concurs with the sentiments expressed by both employees and employers that security certifications are an extremely valuable component of the equation for career development, advancement from IT into management, and securing an individual's future in the profession.

FIGURE 12

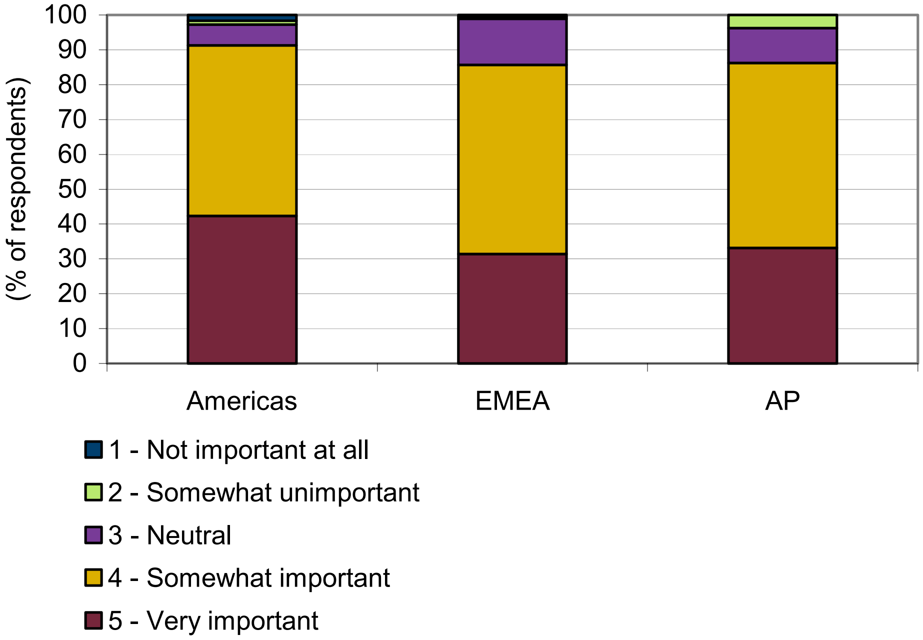
Importance of Information Security Certifications When Hiring Information Security Professionals



Source: IDC's *Global Information Security Workforce* Study, 2005

FIGURE 13

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

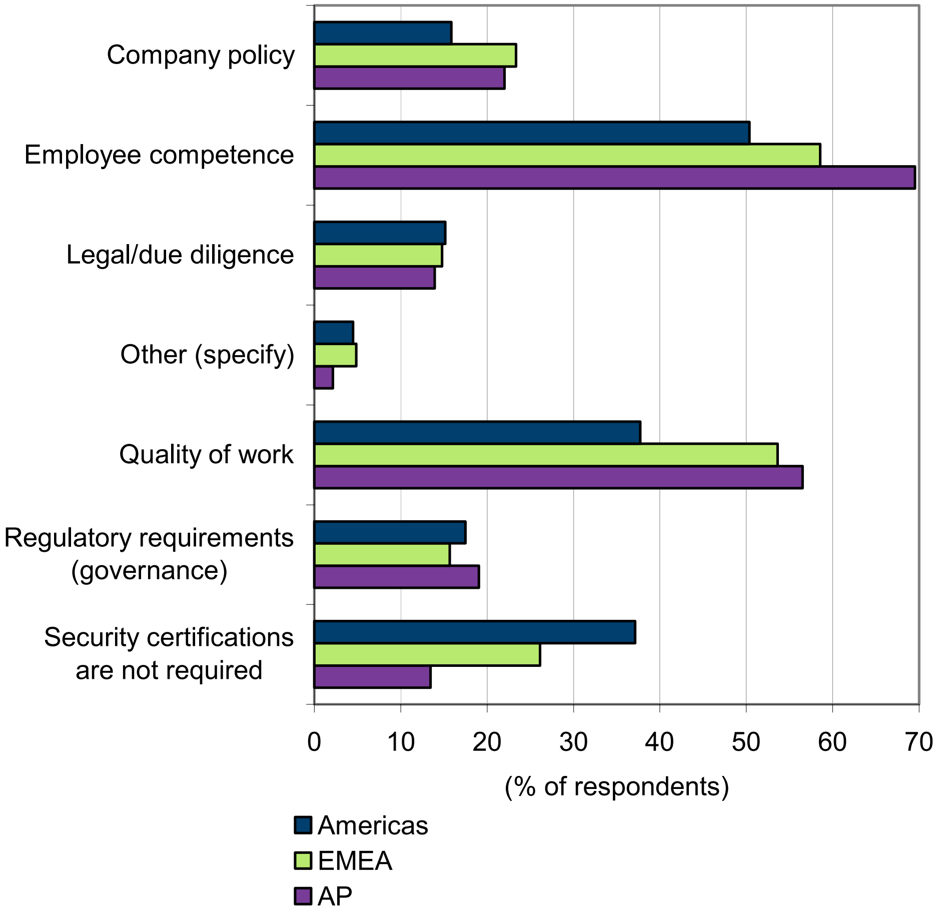


n = 1,431

Source: IDC's *Global Information Security Workforce Study*, 2005

FIGURE 14

Reasons Managers Prefer Hiring Information Security Professionals with Information Security Certifications by Region



n = 4,181

Note: Multiple answers were allowed.

Source: IDC's *Global Information Security Workforce Study*, 2005

FUTURE OUTLOOK

Employees and employers alike have clearly expressed their support for information security certifications. Continuing education plays an important role in enabling individuals to prepare and achieve the differing levels of certification from basic or entry-level to more advanced specialization. Based on the responses from security managers involved in hiring staff, employees are justified in believing that certifications will play an important role in their future. On average, 86% of respondents said that security certifications would be either somewhat or very important to their career advancement. Information security professionals in Latin America and Central Europe, Middle East, and Africa placed more emphasis on the importance of certifications than their colleagues in other regions.

For security professionals to ensure their future in the industry, and the security of their organizations, they must stay on top of the latest technology advancements and regulatory developments, identify how those changes will impact the risk to their organizations, and determine the best solution(s) for mitigating that risk. To accomplish these tasks and translate the technology risk into business risk, security professionals must be armed with business acumen and technology-savvy capabilities.

Tackling critical, emerging areas of security concern will not be an easy problem to solve. To be best equipped for the tasks, information security professionals are looking for additional training and education in the areas of business continuity, forensics, and information risk management, to name a few. Tables 4 and 5 compare areas of interest from last year and this year, in addition to providing some regional insight into the varying topics of interest from the security professional's perspective.

TABLE 4

Top 10 Next Frontiers for Information Security Training and Certification Worldwide, 2004 and 2005

2004	% of Respondents	2005	% of Respondents
Security management practices	48.1	Business continuity and disaster recovery planning	50.5
Telecommunications and network security	47.9	Forensics	50.3
Business continuity and disaster recovery planning	46.3	Information risk management	48.0
Auditing	43.9	Auditing	42.4
Law, investigations, and ethics	43.3	Security management practices	41.3
Applications and system development security	42.2	Access control systems and methodology	39.2
Access control systems and methodology	41.3	Law, investigations, and ethics	39.0
Security architecture and models	36.8	Applications and system development security	38.7
Privacy	36.8	ISO/IEC 17799 (Code of Practice for Information Security Management)	37.3
Operations security	29.9	Security architecture and models	34.6

n = 4,220

Note: Multiple answers were allowed.

Source: IDC's *Global Information Security Workforce Study*, 2005

TABLE 5

Top 5 Areas of Interest for Additional Security Training by Region

Americas	EMEA	AP
Forensics	ISO/IEC 17799 (Code of Practice for Information Security Management)	Business continuity and disaster recovery planning
Business continuity and disaster recovery planning	Information risk management	Forensics
Information risk management	Business continuity and disaster recovery planning	ISO/IEC 17799 (Code of Practice for Information Security Management)
Auditing	Security management practices	Information risk management
Security management practices	Forensics	Auditing

n = 4,220

Note: Multiple answers were allowed.

Source: IDC's *Global Information Security Workforce Study*, 2005

Since 2004, business continuity and disaster recovery planning, forensics, and information risk management have moved to the top of the priority list for advanced education. Auditing appeared on the radar for security professionals in the Americas and AP, while individuals from both the Americas and EMEA expressed interest in security management practices. Security professionals outside the United States stated that getting a better understanding of the ISO/IEC 17799 standard is a top 5 topic. Some topics mentioned that need further attention by providers of education and training are compliance, identity management, and wireless.

When asked if they planned to attain additional security certifications in the next 12 months, more than 60% of security professionals indicated that they intend to acquire at least one more certification. The regional areas with stronger-than-average intent were Latin America and Central Europe, Middle East, and Africa. Both vendor-neutral and vendor-specific certifications will be targeted by security professionals for additional skills and capabilities to transfer into the workplace. A sample of certifications on the priority list for security professionals over the next year include BS7799 Auditor, Cisco Certified Security Professional (CCSP), Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP) and CISSP Concentrations (e.g., Information Systems Security Architecture Professional [CISSP-ISSAP]), GIAC Certified ISO-17799 Specialist (G7799), and Microsoft Certified Systems Engineer: Security (MCSE).

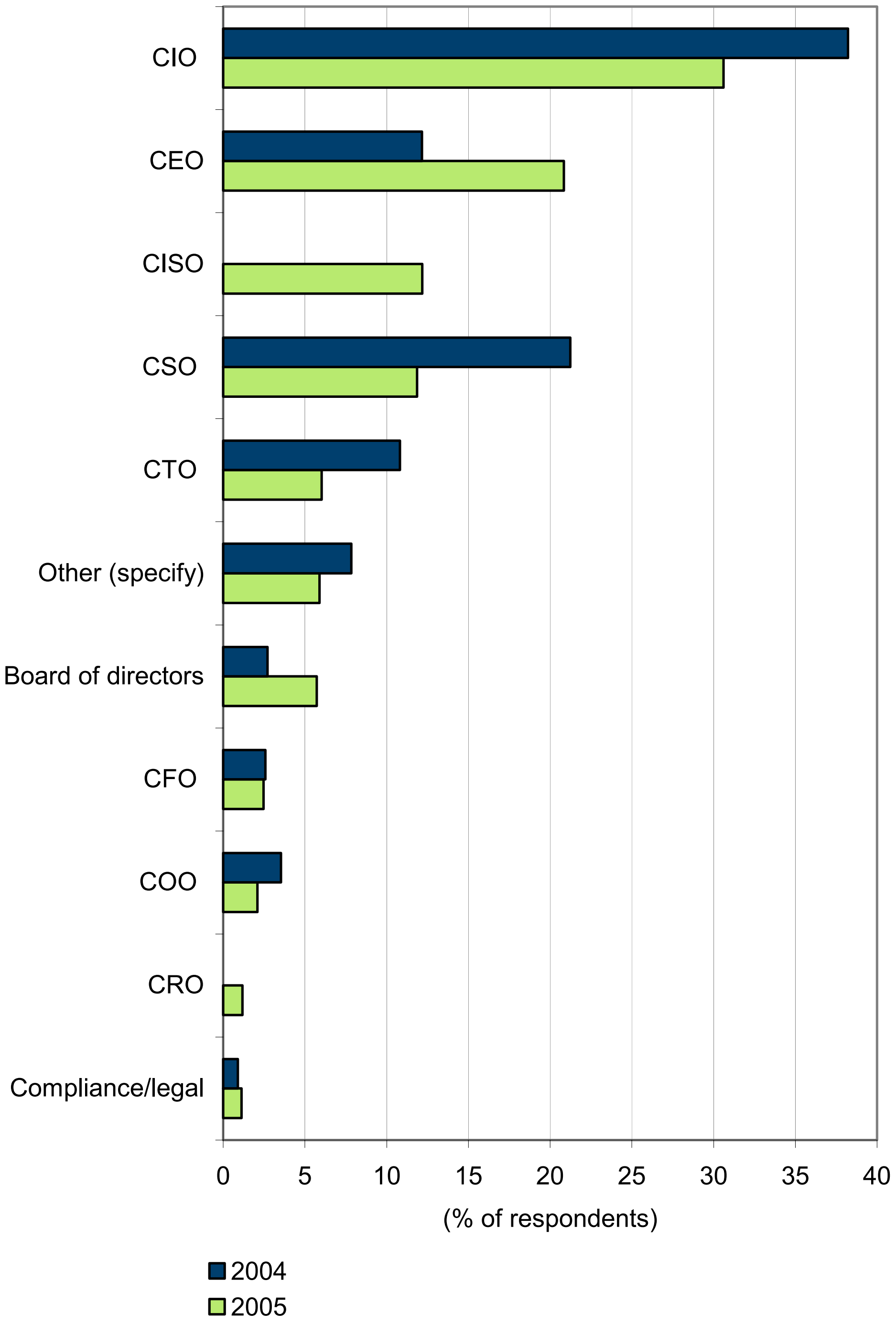
Looking ahead as to how organizations are positioning security accountability, we found that less emphasis is being placed on the CIO and more responsibility and accountability is being designated to the CEO, CSO, and CISO (see Figure 15). The CISO and the CRO (chief risk officer) were new titles added to this year's list of executives based on their emergence in position within the C-suite. Two areas gained more accountability for security in 2005: the CEO and board of directors. Both have ultimate oversight and responsibility for understanding all risk and deciding which risk to mitigate and what level of risk to accept. The changing regulatory environment is one of the primary driving forces causing this noticeable shift in accountability. IDC expects this accountability shift to continue throughout the next couple of years as information security becomes more relevant in the risk management and IT governance strategies of organizations.

According to respondents, some of the shift in responsibility and accountability can be attributed to their actions and influence. In the past year, information security professionals believe that they have made an impact on how security is perceived among LOB owners and executive management. More than 70% said information security's level of influence on LOBs and management has increased slightly or significantly. Less than 3% of individuals thought that security's influence had decreased. Further evidence of this trend has been illustrated as information security professionals are increasingly being asked to participate in meetings about new business solutions and/or initiatives. For security professionals, having a seat at the table in the beginning has proven to be more cost-effective and productive than being brought in after the fact.

Professionals seem confident that their influence will continue into the foreseeable future. Seventy-three percent (73%) of security professionals believe that information security's level of influence on LOBs and executives alike will have increased by next year, a 3% gain. This sentiment was shared across all professionals from various regions of the world. IDC has no reason to doubt the positive outlook provided by the information security professionals surveyed in this study.

FIGURE 15

Individual with Ultimate Accountability for Organization's Information Security Functions



n = 4,247

Source: IDC's *Global Information Security Workforce Study*, 2005

CONCLUSION

Information security professionals from around the globe weighed in with their opinions and viewpoints on the state of the information security profession. From the 4,305 respondents representing 81 countries, we gained a clearer understanding of how professionals are compensated, how their organizations view security, and what the next steps might be to further advance their careers and the profession. The insights shared by these security practitioners are invaluable as IDC draws the following conclusions based on this year's study:

- CEOs and CISO/CSOs are being held more accountable for the security and risk management strategies of their organizations.
- Reporting relationships for security executives and their staffs remain in transition. Organizations across geographies, sizes, and industries have been inconsistent in their methodologies and positioning of information security.
- The information security profession continues to mature, as exemplified by stable compensation practices, greater visibility and influence with management, and higher educational achievements.
- The need for business acumen to augment technical prowess is being heard by the profession, but practitioners and their employers must allocate the time and resources to further promote career development and job satisfaction.
- Providers of information security certifications need to keep pace with the growing demands for knowledge on emerging areas with increasing importance to their constituents, such as risk management and business continuity planning. It is their responsibility to keep raising the bar for practitioners to push the profession to the next level.
- Regions such as Latin America; Central Europe, Middle East, and Africa; and AP offer growing opportunities for security professionals and providers of information security training and education.

Copyright Notice