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

(ISC)2 Information Security Global Workforce Study

Sponsored by: (ISC)^2

Allan Carey

October 2004

IDC OPINION

The information security profession has come a long way over the past five years. From the basement to the executive management suite, information security professionals are more important than ever to the daily operations of modern-day organizations of all kinds. At the same time, roles, responsibilities, and skill sets of these professionals have changed to address the dynamic nature of security technologies, policies, business processes, and organizational risks. This study is designed to capture the current status of the information security professional community and identify the next frontiers it will face. IDC believes the information security profession will undergo more extensive changes as organizations better align themselves to mitigate operational risks due to the following:

IDC believes the information security profession will undergo more extensive changes as organizations better align themselves to mitigate operational risks.

- Adoption of new technologies and services that enable more efficient and profitable, while reliable, means of conducting business
- Shifts in the types of labor pools utilized across organizations around the globe
- Evolution of threats and attacks from a multitude of sources as they become more targeted and have more of an impact
- Convergence of IT security with areas such as physical security and internal risk management to become more of a business function than just a technology function

IN THIS STUDY

Methodology

The *Information Security Global Workforce Survey* was conducted during the late spring/early summer of 2004 on behalf of the International Information Systems Security Certification Consortium (ISC)^2, a nonprofit organization that creates, maintains, and administers international standards for the information security profession. With this study, (ISC)^2 chartered IDC with providing detailed insight into the important trends and opportunities in the profession worldwide. The objective is to provide meaningful research data about the information security profession for the first time to professionals, corporations, government agencies, (ISC)^2 constituents, academia, and other interested parties. The survey was conducted via a Web-based portal, with traffic driven to the site through the use of email solicitations. IDC

IDC surveyed 5,371 respondents from companies and public sector organizations around the globe.

surveyed 5,371 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.

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
- A security engineer or above in title

Respondent Profile

The respondents represent organizations of various sizes, different vertical industries, and varying core competencies and skill sets from more than 80 countries around the world (see Figure 1). However, one common thread among the regional respondents in the Americas; Europe, Middle East, and Africa (EMEA); and Asia/Pacific (AP) was their daily participation in information security activities. Not surprisingly, almost three-quarters of the responses came from the Americas, which contains a high concentration of security talent, particularly within the United States. Each respondent had a role in purchasing, managing, or maintaining a multitude of IT security technologies, services, and/or personnel.

Each respondent had a role in purchasing, managing, or maintaining a multitude of IT security technologies, services, and/or personnel.

In terms of functions, most respondents were at the security engineer level or higher within their organization. More than a quarter of the respondents were security consultants (i.e., the individuals who are on the frontlines, daily speaking to and advising organizations on their security strategies and challenges). Almost 10% of executive management weighed in with their opinions on the information security profession, with the remainder consisting of various security titles (see Figure 2).

With titles such as 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.

Organization Size

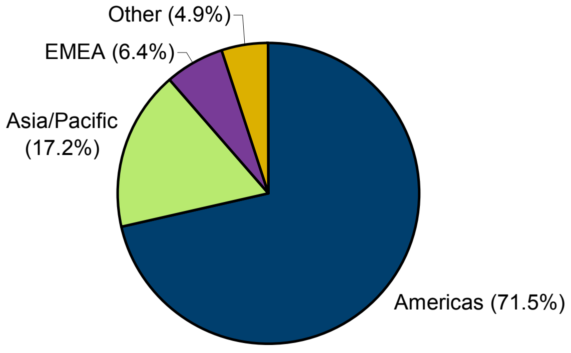
Organizations of assorted sizes participated in the survey. For segmentation purposes, organizations were split into multiple categories (see Figure 3). More than 65% of responding organizations had more than 1,000 employees, while 17.1% from smaller organizations had fewer than 100 employees. The remainder would be considered the midmarket or medium sized.

More than 65% of responding organizations had more than 1,000 employees.

In addition to being asked about the size of their organizations, respondents were asked about their organizations' annual revenue. Almost 45% of the responding organizations generated more than $1 billion in annual revenue. Another 36% had less than $100 million in revenue generation (see Figure 4).

FIGURE 1

Respondents by Geographic Region

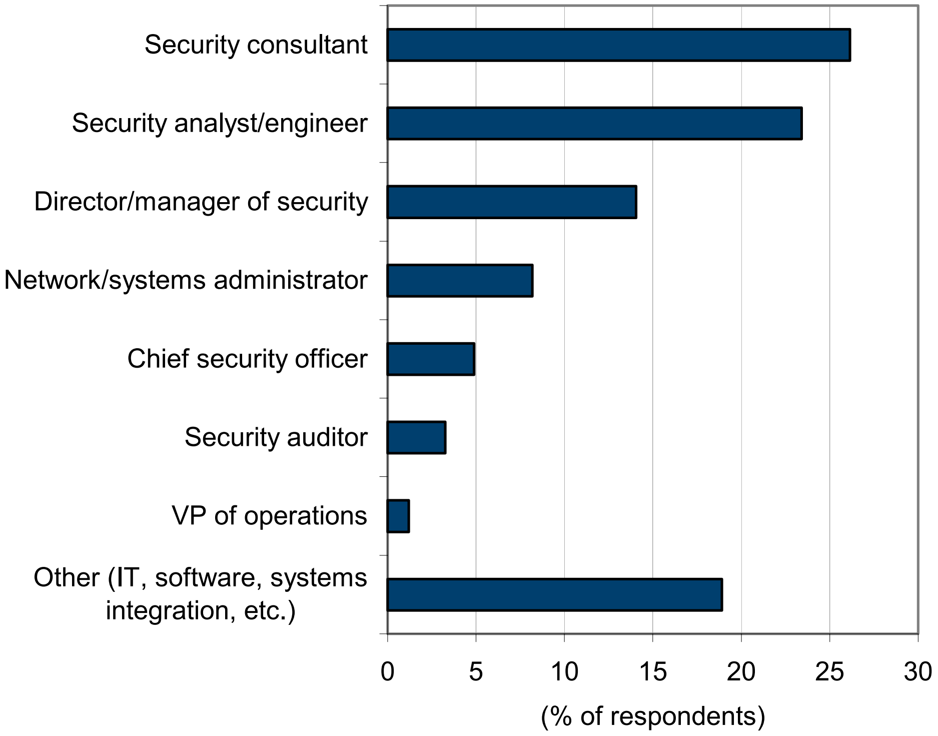


n = 5,371

Source: IDC's *Information Security Global Workforce Survey,* 2004

FIGURE 2

Respondents by Job Function

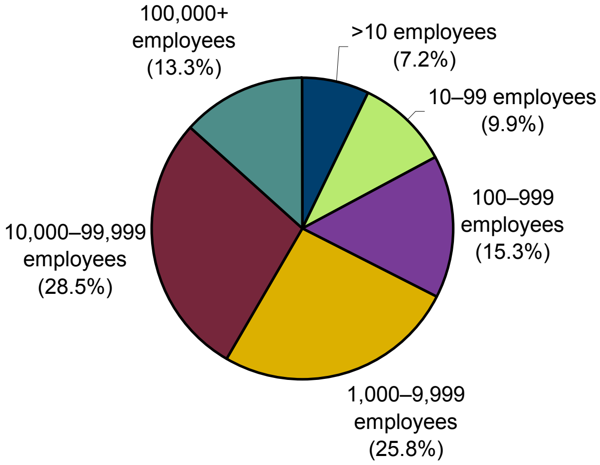


n = 5,321

Source: IDC's *Information Security Global Workforce Survey,* 2004

FIGURE 3

Respondents by Company Size

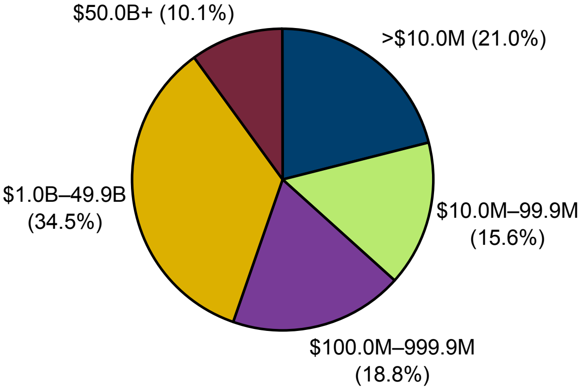


n = 5,285

Source: IDC's *Information Security Global Workforce Survey,* 2004

FIGURE 4

Respondents by Company Revenue



n = 5,170

Source: IDC's *Information Security Global Workforce Survey,* 2004

Industry

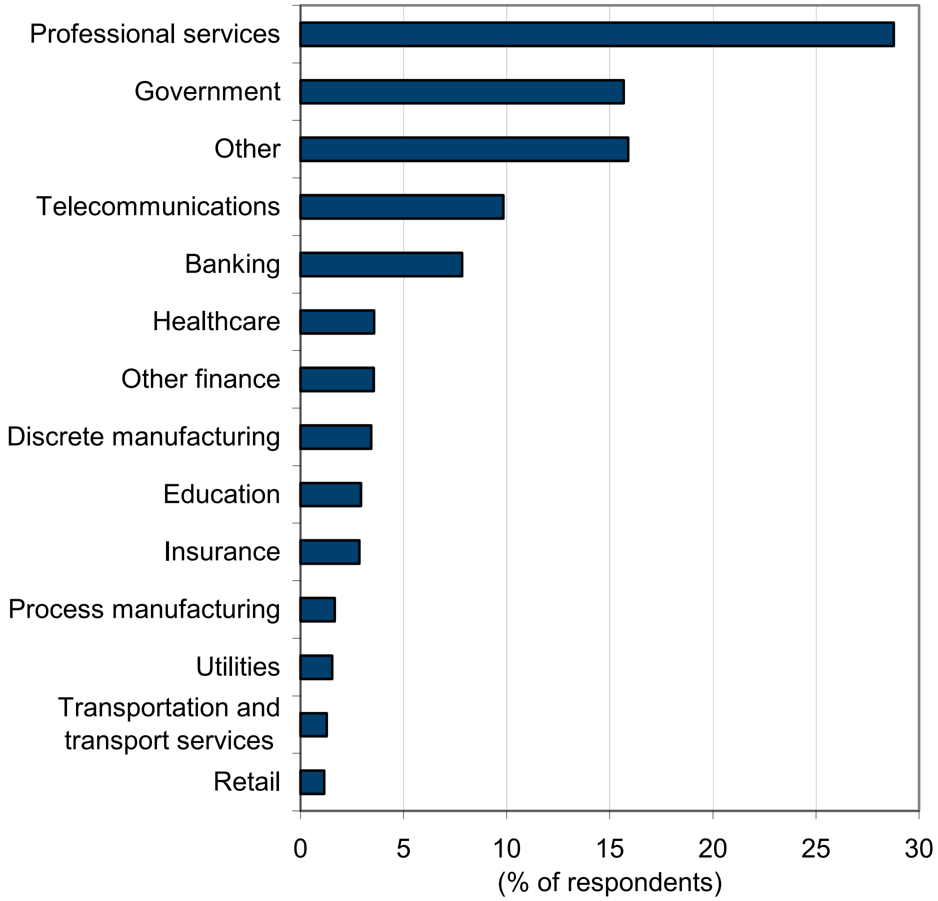
Organizations from both the public and private sectors were represented and provided valuable feedback. Banking, healthcare, government, manufacturing, and utilities were just a few of the responding industries with increasing security requirements and challenges (see Figure 5). The professional services industry, consisting primarily of security consultants, was the largest segment; it was followed by the government sector.

Banking, healthcare, government, manufacturing, and utilities were just a few of the responding industries with increasing security requirements and challenges.

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 5,371 individuals surveyed for this IDC study.

FIGURE 5

Respondents by Vertical Industry



n = 5,371

Source: IDC's *Information Security Global Workforce Survey,* 2004

Executive Summary

Introduction

Ubiquitous connectivity to the computing infrastructure from external and internal sources has dramatically changed the way organizations communicate, operate, and transact on a daily basis. Hence the need for increased protection of intellectual property, organizational assets, customer data, and stakeholders has become a boardroom issue and top priority. Vulnerable systems present enticing opportunities for computer hackers, current and past employees, contractors, and competitors to compromise or destroy proprietary information within the system(s) or to otherwise disrupt the normal operation of the system(s).

Vulnerable systems present enticing opportunities for computer hackers, current and past employees, contractors, and competitors to compromise or destroy proprietary information.

IT staff are the frontline firefighters in the battle against cybercrime and other malicious activity. Proper education and continuous training are essential elements to the successful execution of their position. Their role requires an effective combination of networking experience, security knowledge, and business acumen. For those organizations staffing up to address security concerns, distinguishing one individual's knowledge, skills, and qualifications from another's can be difficult. Certifications have become one of the main differentiating elements when a group of individuals' (such as doctors, accountants, and lawyers) qualifications are being evaluated and compared.

Objectives and Overview

The major objectives of this survey were to provide an annual "barometer" of the information security professional environment, establish a quantifiable context of the information security profession, serve as a career guide, and identify important trends and opportunities within the profession.

IDC received responses from 5,371 decision makers and influencers from organizations worldwide regarding their perceptions of the information security profession. Respondents were from organizations of all sizes, including small (1–99 employees), medium-sized (100–999) and large (1,000 and above). In addition, respondents were from various industries, including financial services, government, healthcare, telecommunications, and transportation. Results were analyzed from a regional perspective.

The Information Security Community

Escalation of logical and physical security concerns within public and private sectors has driven interest in security training and education programs, not only in the United States but in all regions of the world. This signals a shift in emphasis from the past focus on technology solutions to secure the organization to a more holistic approach that addresses people, processes, and policies. IDC believes spending on information security training and education in the United States alone is expected to reach approximately $1 billion by 2006, representing 16% year-over-year growth, which will result in better-educated corporate citizens who do their part to proactively protect the organization.

Escalation of logical and physical security concerns within public and private sectors has driven interest in security training and education programs.

One important aspect of IT training is maintaining, refreshing, and retooling the skills of the staff. As IT professionals seek new ways to differentiate themselves from their colleagues, to challenge themselves and further their careers, areas of specialization such as security have and will continue to become increasingly attractive and valuable. As the demand in recent years for these specific skill sets and capabilities has outpaced the demand for more generalized IT knowledge, the population of IT security professionals has grown.

IDC predicts the worldwide population of information security professionals will grow to more than 2.1 million professionals in 2008, representing a 13.7% compound annual growth rate (CAGR) over the next five years from the estimated 1.15 million in 2003.

IDC predicts the worldwide population of information security professionals will grow to more than 2.1 million professionals in 2008, representing a 13.7% compound annual growth rate over the next five years from the estimated 1.15 million in 2003.

From a regional perspective, with approximately 313,000 IT security practitioners in 2003, the Asia/Pacific market is posed for impressive growth to more than 720,000 by 2008, representing a CAGR of 18.3% over the forecast period. The opportunity for information security professionals within the Americas, in particular the United States, remains more robust in terms of overall total security spending. Even though the AP market, including Japan, may not be as large as other regions of the world, this region exhibits attractive opportunities for professional information security talent.

In 2008, the Americas, with 36.1% of the market, will compose the largest market opportunity in terms of information security staffing. AP, with a third of the market, will follow. Combined, these markets will account for more than 70% of the worldwide information security population. Information security professionals worldwide and their communities will continue to be affected by changing regulatory requirements, emerging technologies, and advancement of the threat environment in addition to traditional business factors, such as profits, revenue generation, and productivity.

Our research of this community revealed its diversity across industries, responsibilities, and salaries but disclosed many similarities in educational background, experience levels, and future needs. In fact, the study highlighted the following trends for the surveyed men and women in the information security profession:

- Carry a variety of titles, including security consultant, security manager, director of security, and chief information security officer, with the majority of respondents being male

- Possess an average of 13 years of general IT experience, along with an average of 7 years of security experience

- Hold multiple security-related certifications, including one vendor-neutral and one or more vendor-specific certifications

- Receive an average of 10 days of information security–related training each year

The Internal Security Organization

Within the typical internal IT department (depending on the size of the organization), there is either a group of individuals or an individual responsible for the IT security of the entire organization. According to representatives from responding organizations, the internal information security group:

- Employs an average of 10 full-time information security professionals and 5 part-time staff members
- Typically (more than one-third of the time) reports into the IT department
- Derives ultimate direction from the chief information officer (in 40% of the situations)

Certifications

For 92% of security hiring managers, certifications are important when hiring decisions are being made. Security hiring managers cite several primary reasons they prefer internal security to obtain and keep current certifications. First and foremost, information security certifications attest that an individual has obtained and tested to a predetermined level of knowledge or common body of knowledge in particular security domains. Certifications also extract the guesswork for an employer and afford the employer some degree of comfort or a guarantee as to an individual's competency/knowledge level. In addition, some security hiring managers insist on information certifications as a matter of personal preference. Finally, certification can be critical in terms of legal liability or corporate due diligence.

For 92% of security hiring managers, certifications are important when hiring decisions are being made.

IDC divides information security certifications into two categories: vendor neutral and vendor specific. A vendor-neutral certification, such as Certified Information Systems Security Professional (CISSP) or Certified Information Systems Auditor (CISA), encompasses a broad scope of knowledge and is not tied to any specific technology vendor or product. Vendor-specific certifications, such as Cisco Certified Security Professional (CCSP) or Microsoft Certified Systems Engineer: Security (MCSE), are offered by technology vendors covering knowledge and content about their products, solutions, and best practices. Both kinds of certifications play an extremely important role in the market, fulfilling specific knowledge and learning requirements of IT security professionals, and demonstrate predetermined acceptable levels of competency and experience.

Future Outlook

Independent reports suggest that the global economic recovery is steadily improving. That evidence, coupled with the results of this study, suggests that IT and information security professionals have good reason to be optimistic about the future of their professions. This group tends to be cautiously optimistic.

On a regional level, security professionals in the Americas and EMEA are more optimistic about their potential for career growth than are their colleagues in AP. As they survey the security landscape, a few of the key areas where they see the need for additional training and certification include security management practices,

On a regional level, security professionals in the Americas and EMEA are more optimistic about their potential for career growth than are their colleagues in AP.

telecommunications and network security, and business continuity and disaster recovery planning. Information security professionals see mastery of these topics as not only crucial to continuing education but also necessary to ensure that their certifications remain relevant over the long term. One emerging issue to watch surrounding security certifications is the impact of ISO/IEC 17024. More than 60% of surveyed members of the information security community feel that their information security certifications should be accredited under the new ISO standard accreditation.

The path to the future is not always smooth, and its course is impossible to guarantee. IDC research indicates, however, that information security professionals can remain upbeat about their future prospects for advancement and career satisfaction.

SITUATION OVERVIEW

The proliferation and growth of organizational intranets and extranets and the increasing importance of ecommerce have dramatically increased the openness and accessibility of computer networks. With this openness, the Internet has become a widely accepted platform for many business-to-business, direct-to-customer, government-to-citizen, and evolving indirect-to-consumer transactions.

The proliferation and growth of organizational intranets and extranets and the increasing importance of ecommerce have dramatically increased the openness and accessibility of computer networks.

Consequently, organizations are more dependent than ever before on permitting all stakeholders (e.g., customers, citizens, suppliers, partners, and employees) access to the infrastructure. This continuously available environment allows organizations to leverage their existing network infrastructures to gain a competitive advantage, achieve greater market share, streamline operational processes, and reach or develop strategic alliances to further expand their breadth of offerings.

Although organizations can realize many advantages through collaborative computing environments, and businesses and governments are heavily dependent on them, the accessibility and the relative anonymity of users make these systems, including the information that resides on them, vulnerable to a variety of security threats. Vulnerable systems present enticing opportunities for computer hackers, current and past employees, contractors, competitors, or government enemies to compromise or destroy proprietary information within the system or to otherwise disrupt the normal operation of the system. Furthermore, open computing environments are complex and typically involve a heterogeneous selection of network hardware, operating systems, and applications supplied by a multitude of vendors, making these networks difficult to manage, monitor, and protect from unauthorized access.

This escalation in security issues has driven interest in security training and education programs, not only in the United States but in all regions of the world. IDC believes spending on information security training and education in the United States alone is expected to reach approximately $1 billion by 2006, representing 16% year-over-year growth (see *Worldwide and U.S. Security Services 2004–2008 Forecast,* IDC #31054, April 2004). Overall, the delayed recovery in IT spending in 2003 and so far in 2004 has strongly affected the global IT training market. This decrease has resulted in delays in new projects, a decline in new software licenses for many software vendors, and the inability to predict training expenditures in general. Bubbling beneath a surface of slow industry growth, however, are pockets of higher-growth opportunities, such as security training, which will represent a significant opportunity for career advancement and job growth for several years to come.

Based on a multitude of factors, including organization size, IT budget, and vertical industry, IDC estimates the number of information security professionals worldwide in 2004 to be 1.3 million, a 14.5% increase over 2003. This figure is expected to increase to more than 2 million by 2008, displaying a CAGR of 13.7% from 2003 to 2008 (see Table 1).

IDC estimates the number of information security professionals worldwide in 2004 to be 1.3 million, a 14.5% increase over 2003.

TABLE 1

Worldwide Information Security Professionals by Region, 2003–2008

	2003	2004	2005	2006	2007	2008	2003–2004 Growth (%)	2003–2008 CAGR (%)
Americas	448,883	507,498	572,732	642,864	714,865	792,785	13.1	12.0
EMEA	393,485	443,461	497,783	554,917	613,183	676,341	12.7	11.4
Asia/Pacific	313,446	372,810	441,073	522,560	617,666	727,611	18.9	18.3
Total	1,155,814	1,323,769	1,511,589	1,720,341	1,945,714	2,196,737	14.5	13.7

Notes:

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 organization size, business model, industry, and IT budget.

Interest in gaining IT security specialization by IT professionals will continue throughout the forecast period.

Government and the private sector will promote programs to attract new talent to the information security profession.

Organizations will always require internal IT staff dedicated to security activities.

Asia/Pacific remains a growth area for high tech and will attract individuals to meet the demand.

Source: IDC, 2004

Incremental but healthy growth is anticipated during the forecast period due to a number of drivers in the marketplace:

- **Government regulations.** The regulatory environment is becoming more intense as legislation is passed that increases specific security implications for industries and organizations in general.

- **New technologies.** Communications methods, such as instant messaging, wireless, and the adoption of voice over IP and Web services, have implications on corporate security. Many of these technologies will drive the demand for architecture and design competencies as well as security strategy and planning.

- **Threat focus.** Proactive security, such as risk management, patch management, and secure application testing and development can help alleviate the pain many organizations experience.

Industry Trends and Challenges Associated with Information Security

The pace of technological change and infrastructure transformation is staggering as organizations build and modify processes and systems to achieve strategic objectives and goals. Removal and addition of software, hardware, services, and users to enable these changes creates an extremely complex environment to manage, control, and protect. Organizations require business continuity, 24-hour network availability, and applications access to maintain employee productivity. Any disruption to normal operations could be catastrophic to the performance of services supplied by any business unit or government agency. These are a sample of the influencers shaping the information security industry. Other factors include:

- The costs associated with security breaches are high.
- Creators of blended threats and attacks are playing cat and mouse with IT vendors and their customers.
- Security is increasingly requiring a more proactive than reactive approach.

Market Developments Causing an Increase in Information Security Certifications

Organizations cannot protect the integrity, confidentiality, or availability of information in today's highly networked systems environment without ensuring that each member of the organization understands his/her role and responsibilities and is adequately trained to perform them. Addressing the human factor is critical to success. Therefore, as organizations realize the important role every member must play in securing the organization, the following factors are beginning to occur simultaneously in the marketplace:

- Employers are seeking individuals with a foundation of knowledge as well as experience.
- IT professionals are looking for ways to differentiate themselves through specialization in areas such as security.
- The market is more greatly rewarding those IT professionals with certifications than those without.

Security Workforce Profile

Throughout the past five years of IT, one sector remained strong, both during and after the dot-com era — security. Security professionals experienced growth in job prospects, career advancement, higher base salaries, and salary premiums for certification at faster rates than other areas of information technology. That's not to say there wasn't a change in the job descriptions, requirements, and qualifications to become a practitioner of information security to reflect the changing business demands. The requirements and qualifications necessary to be an information security professional have changed just as drastically as the technology employed on a daily basis.

Security professionals experienced growth in job prospects, career advancement, higher base salaries, and salary premiums for certification at faster rates than other areas of information technology.

Overwhelmingly, the majority of respondents (88.9%) were male. This figure did not vary significantly from region to region. The highest female response (12.7%) came from the Americas. EMEA and Asia/Pacific were very similar, with more than 90% of survey responses coming from men. It is widely known that the IT profession consists primarily of men, but programs are emerging at both the enterprise and academic levels, such as the Executive Women's Forum and Women in Security, to foster career development of women information security professionals and to stimulate greater female interest in the information security profession.

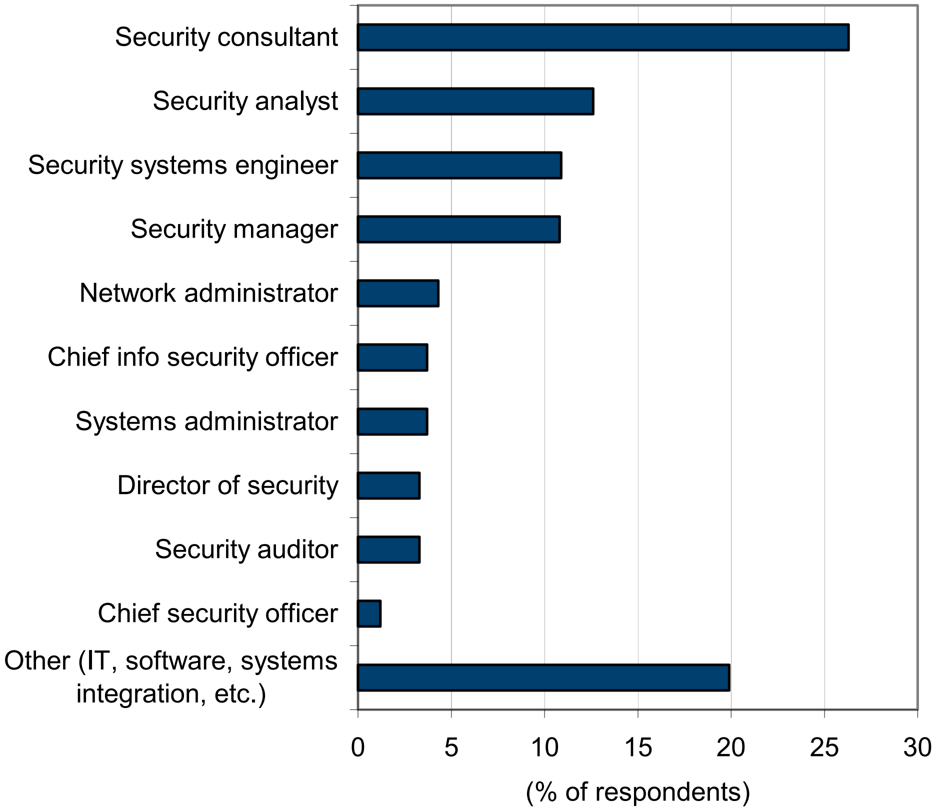
The men and women of information security carry a variety of titles within their respective organizations. From security engineers and analysts to chief security officers, all play a vital role in the way organizations protect themselves and mitigate risk (see Figure 6).

From security engineers and analysts to chief security officers, all play a vital role in the way organizations protect themselves and mitigate risk.

Of the individuals surveyed, 21% are responsible for managing their organization's IT staff, 32% are responsible for managing the organization's security staff, and 42% are involved in making information security staff hiring decisions.

FIGURE 6

Titles of Information Security Professionals



n = 5,321

Source: IDC's *Information Security Global Workforce Survey,* 2004

Experience Counts in Security

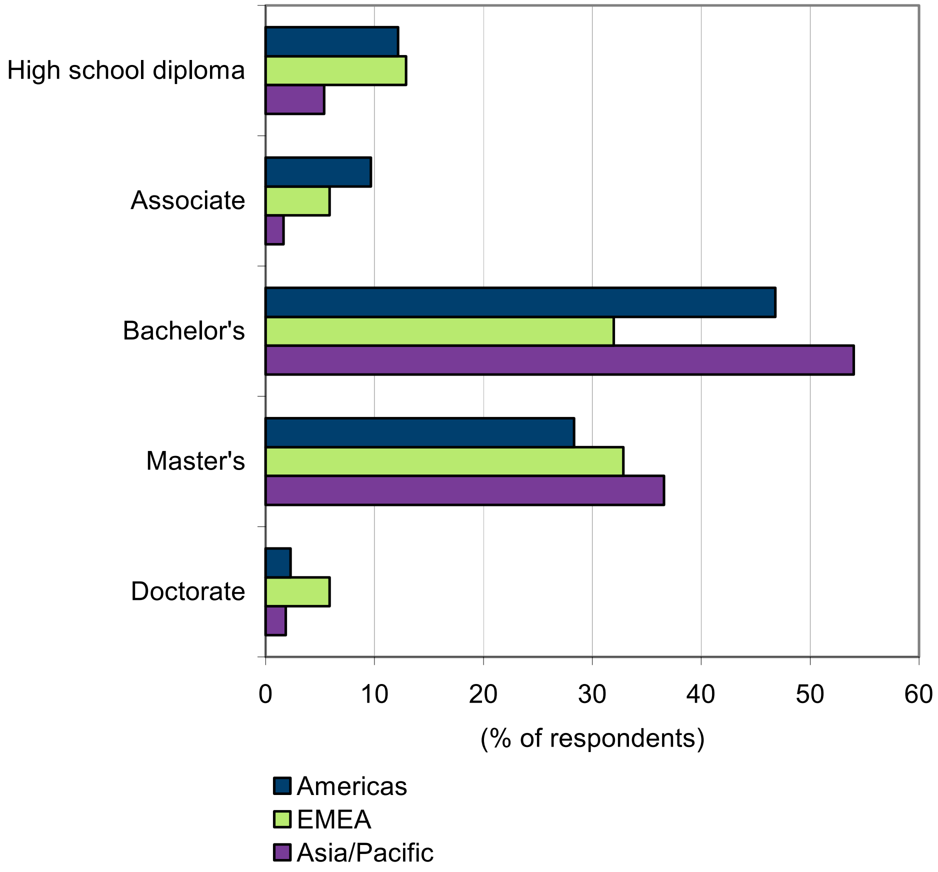
On average, survey participants have 13 years of general IT experience, along with an average of 7 years of security experience. Respondents felt that it is as important to understand general networking and IT as it is to grasp the security component. In the Americas, the average information security professional has been in the IT industry for 14 years, while experience among EMEA and AP security practitioners was slightly less than in the Americas: 12 years and 9 years, respectively. The average security professional across each region has been in the industry for 8 years (Americas), 6 years (EMEA), and 5 years (AP).

On average, survey participants have 13 years of general IT experience, along with an average of 7 years of security experience.

More than 80% have undertaken some degree of higher education in the form of either a bachelor's, master's, or doctorate. In a comparison of education levels on a regional basis, a greater percentage of Asia/Pacific information security professionals than professionals in other areas of the world possessed a college-level education. Greater than 90% of AP respondents had attained a bachelor's or higher (see Figure 7).

FIGURE 7

Highest Level of Education Obtained by Information Security Professionals by Region



n = 5,312

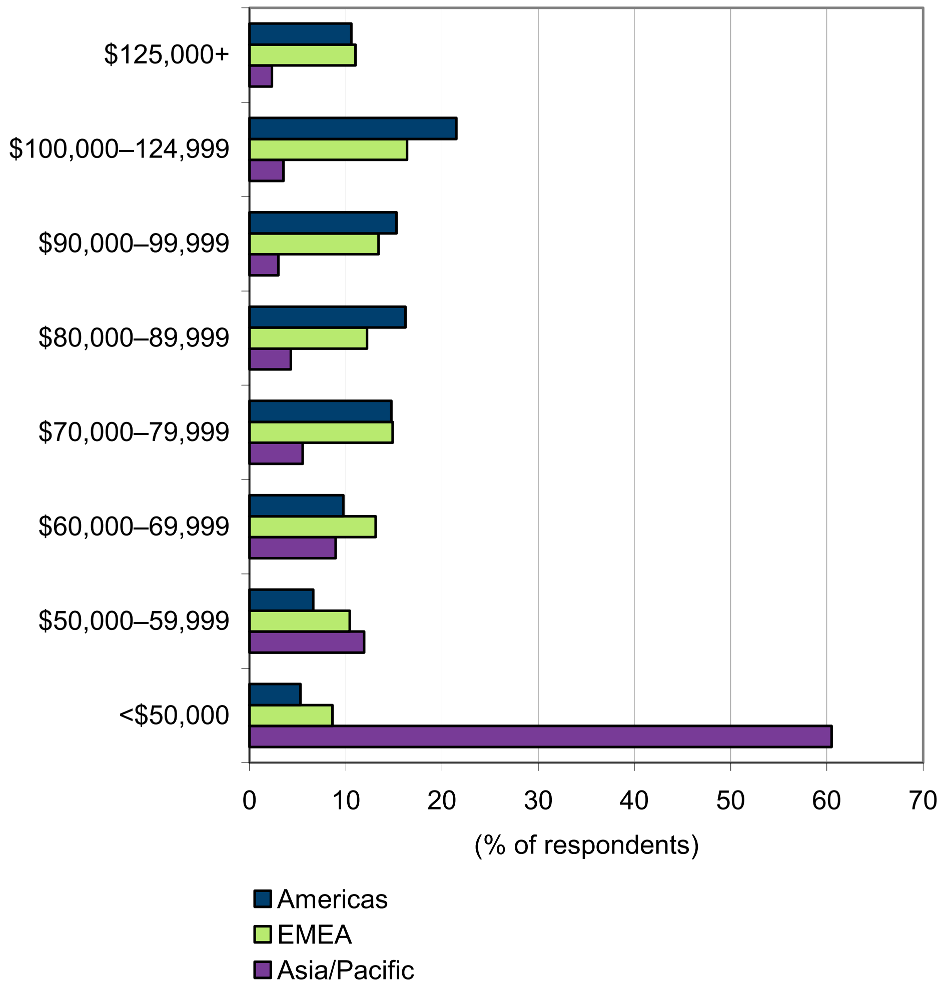
Source: IDC's *Information Security Global Workforce Survey*, 2004

Experience and education are two of the most significant factors that employers take into account when they determine an individual's eligibility and salary for a position. Job postings typically state that salary will be commensurate with experience and education. According to survey results, salaries differed widely by region. Figure 8 illustrates the cost advantage of using labor offshore by showing the salary gaps between Asia/Pacific and other regions. More than 70% of AP respondents earn less than $60,000 annually, compared with 12% in the Americas and 19% in EMEA. The lower salaries are indicative not only of the respondents' level of experience but also the general wage structure within this particular region.

Experience and education are two of the most significant factors that employers take into account when they determine an individual's eligibility and salary for a position.

FIGURE 8

Salary Bands for Information Security Professionals by Region



n = 5,263

Source: IDC's *Information Security Global Workforce Survey*, 2004

Credentials and Training

Another factor hiring managers are increasingly taking into consideration when reviewing IT candidates is the candidate's credentials. Credentials can consist of both vendor-neutral and vendor-specific education, including certificates and certifications. By receiving credentials, candidates illustrate their competency in a particular area and differentiate themselves from other candidates who may have similar qualifications.

By receiving credentials, candidates illustrate their competency in a particular area and differentiate themselves from other candidates who may have similar qualifications.

Results from the survey highlighted the fact that many respondents possess multiple certifications, including one vendor-neutral and one or more vendor-specific certifications, in their toolkits. IT staff members often acquire multiple certifications because they need not only a core understanding of security technology and processes but also an understanding of the technologies within their employer's infrastructure environment. Depending on the IT infrastructure and computing environment an organization has built over the years, individual IT staff members carry specific responsibilities and technology ownership, requiring them to obtain the necessary competencies and skills sets to perform their job function successfully. Hence specific technology certifications from vendors such as Microsoft or Cisco may be required in addition to any broader certifications (such as a CISSP).

Technology does not stay stagnant, however. Software and hardware change behavior each time a new version is released, a patch is issued, or a service pack becomes available. Not only does software and hardware's own behavior change, but the way software and hardware interact with other applications and devices changes as well. Consequently, information security professionals must try to keep pace with the ever-changing threat environment and attack methodologies of hackers, insiders, and other vagrant intruders attempting to exploit weaknesses in the software and hardware technologies.

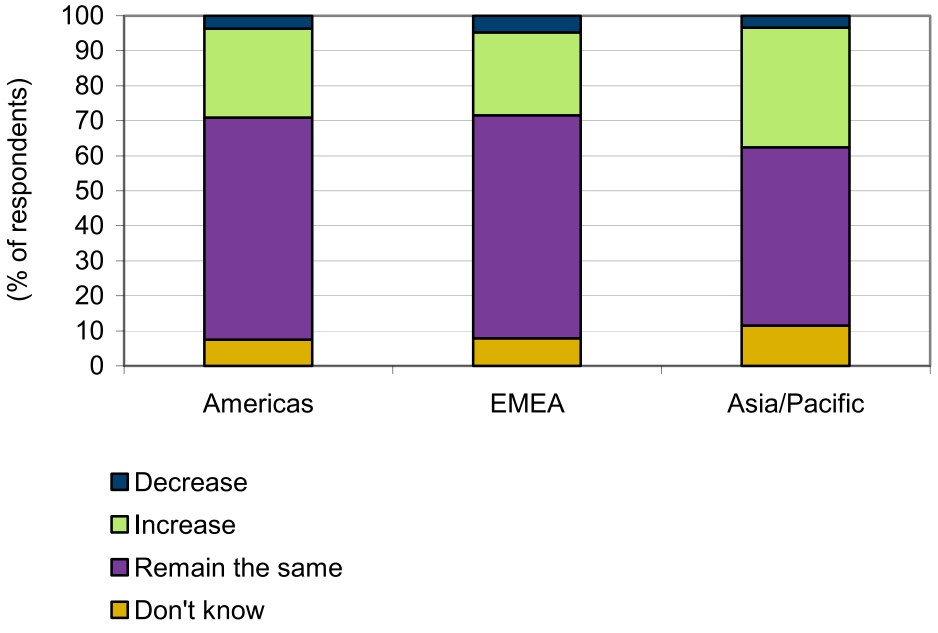
Many have said that software is only as good as its last update. A constant refresh and maintenance of the technology is necessary to ensure peak performance and operational efficiency. The same could be said of the professionals developing, integrating, managing, and maintaining these systems. Their skills and knowledge base must be kept current for them to properly perform in their assigned role and function; otherwise they become obsolete, just as the technology they interact with. This is why IT training has become an important issue for organizations' HR departments and employees alike.

According to the survey results, IT security employees receive an average of 10 days of information security–related training each year. Whether in the Americas or AP, security practitioners received the same amount of training. Information security professionals were cautiously optimistic that the amount of training given during 2005 would increase. The majority, more than 60%, believed the number of training days would stay the same, while another 27% thought it would increase. Opinions on the increase differed by region. Americas-based information security professionals forecast a 100% jump in their training days in contrast to the 50% or 67% jumps predicted by EMEA- and AP-based professionals, respectively. Figure 9 offers more insight into the regional sentiments.

According to the survey results, IT security employees receive an average of 10 days of information security–related training each year.

FIGURE 9

Expected Change in Amount of Information Security–Related Training from 2004 to 2005 by Region



n = 5,042

Source: IDC's *Information Security Global Workforce Survey,* 2004

Security Organization Profile

Organizations employ an average of 10 full-time information security professionals and 5 part-time staff members.

Within the typical internal IT department, depending on the size of the organization, there is typically a group of individuals or one individual responsible for the IT security of the entire organization. As mentioned previously in this document, differing positions within the organization are the result of several factors, including the size of the organization, vertical industry, level of security sophistication, and IT budget. Responding organizations employ an average of 10 full-time information security professionals and 5 part-time staff members. AP was the only region with slightly different requirements; AP organizations employed an average of 9 full-time and 5 part-time information security professionals.

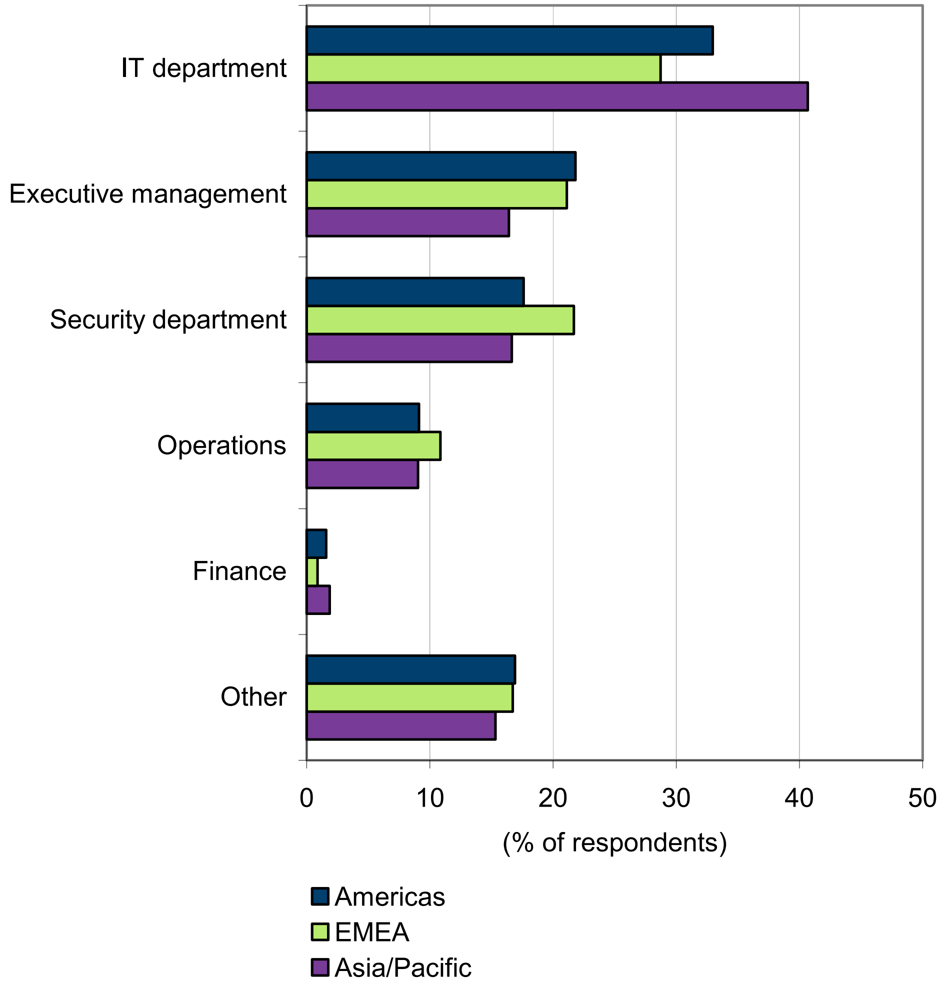
A common question among those within and without the industry is, "Who does the information security group report to?" The answer involves many of the same factors taken into account when the security group is being staffed. Figure 10 illustrates the varying departments within an organization that information security professionals report to and are managed by. For example, in more than 40% of AP-based organizations, the 14 full-time and part-time member security group reports into IT. Equally, 17% of surveyed security professionals report into either executive management or the security department. Interestingly, there was a higher percentage

(21%) of IT security staff reporting to the security department in EMEA-based organizations than in any other region. Across organizations worldwide, however, finance and operations were the least likely groups to have the IT security group reporting to them.

FIGURE 10

Reporting Lines for Information Security Departments by Region

Q. What functional area of your organization do you specifically report into?



n = 5,309

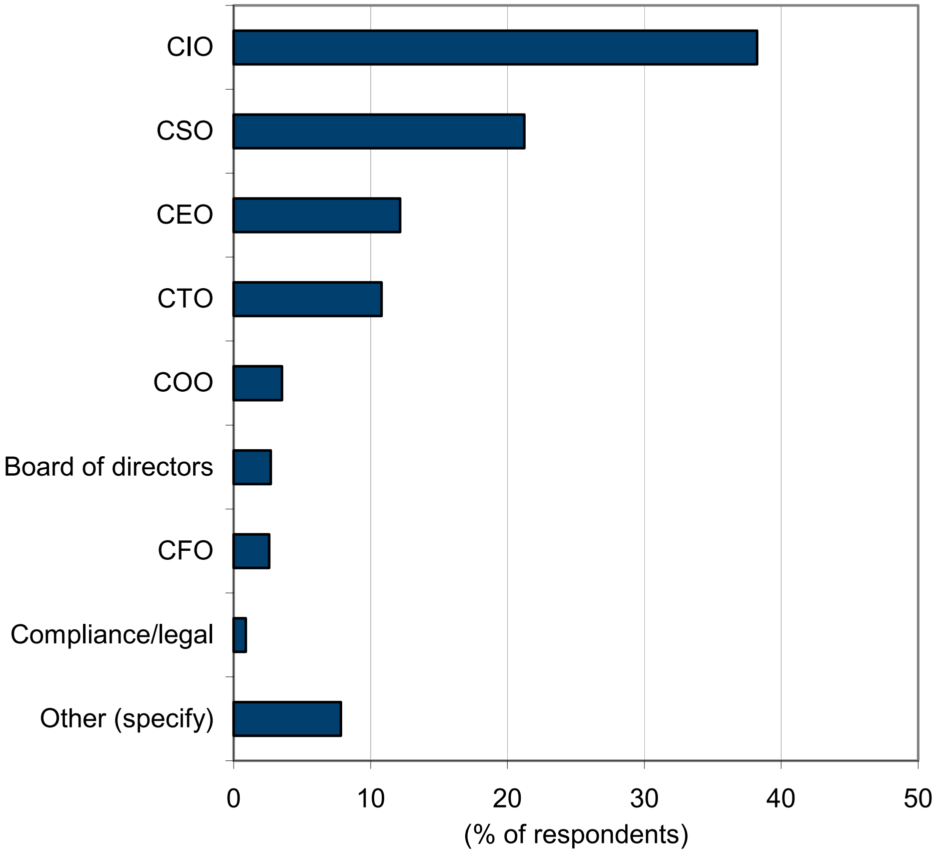
Source: IDC's *Information Security Global Workforce Survey,* 2004

Some of the functional areas mentioned in the "other" segment were consulting/professional services (due to the high response rate of security consultants), audit or internal audit, engineering, and legal/general counsel.

At the end of the day, the person ultimately responsible for the security of the organization is the chief information officer (CIO). Across all regions, in almost 40% of the responding organizations (see Figure 11), the CIO has managing responsibility and decision-making ability for IT security. The second-most-popular choice was the chief security officer (CSO), a position relatively unheard of 10 years ago. The third position belongs to the CEO, who has ultimate responsibility for the entire organization. In each of the regions except the Americas, there were slightly varying orders of choice. For instance, organizations in EMEA have a higher predominance of the CSO (26%), followed by the CIO and CEO, at 21% and 17%, respectively. In AP, the order was similar to the global average, except that the third position went to the CTO by a slim margin.

FIGURE 11

Individual with Ultimate Responsibility for Organization's Information Security



n = 5,025

Source: IDC's *Information Security Global Workforce Survey,* 2004

Status of Security Certifications

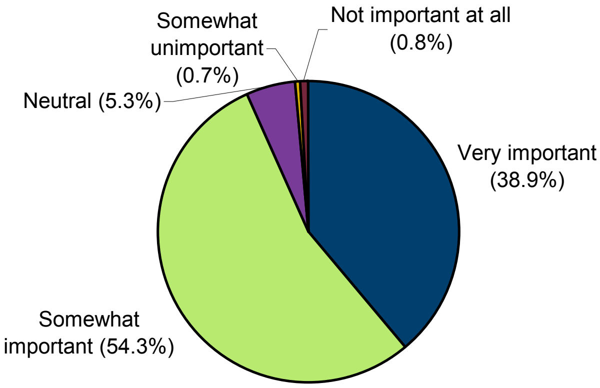
Reasons to Hold Security Certifications

IDC asked the 42% of information security professionals actively involved in making hiring decisions related to their organizations' internal IT security staff about the importance of security certifications. Overwhelmingly, as Figure 12 shows, security hiring managers believe security certifications are either somewhat important or very important when hiring decisions are being made. In fact, an average of 93% of global security managers believe this to be true.

Security hiring managers believe security certifications are either somewhat important or very important when hiring decisions are being made.

FIGURE 12

Importance of Information Security Certifications When Hiring Information Security Professionals



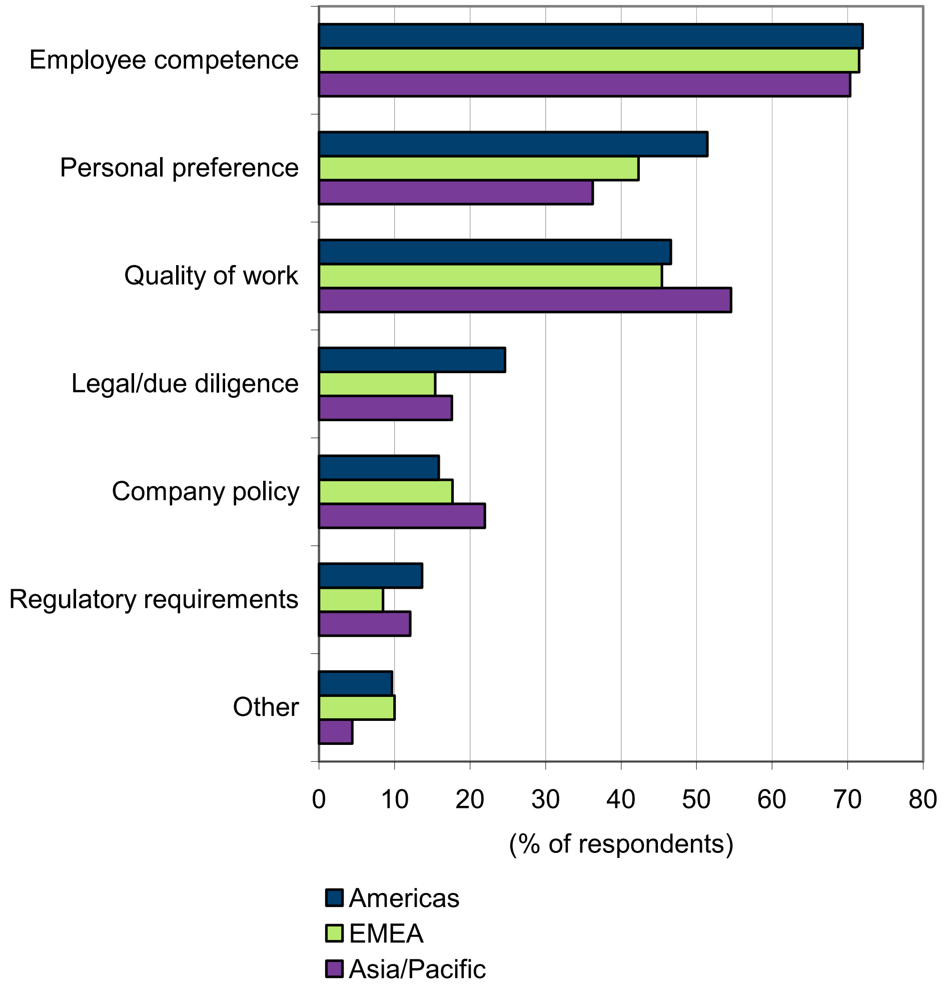
n = 2,133

Source: IDC's *Information Security Global Workforce Survey,* 2004

For 93% of security hiring managers, certifications are important when hiring decisions are being made. Security hiring managers cite several primary reasons they prefer internal security to obtain and keep current certifications. First and foremost, information security certifications attest that an individual has obtained and tested to a predetermined level of knowledge or common body of knowledge in particular security domains. Certifications also extract the guesswork for an employer and afford them some degree of comfort or a guarantee as to an individual's competency/knowledge level. In addition, some security hiring managers insist on information certifications as a matter of personal preference. Finally, certification can be critical in terms of legal liability or corporate due diligence. Quality of work was determined to be a more powerful factor than personal preference in requiring certification in EMEA and AP, unlike those factors influencing hiring decisions of security managers in the Americas (see Figure 13).

FIGURE 13

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



n = 2,108

Note: Multiple responses were allowed.

Source: IDC's *Information Security Global Workforce Survey,* 2004

In the information security world, IDC divides certifications into two categories: vendor neutral and vendor specific.

Many of the survey participants hold multiple certifications as badges of honor. They often have the acronym(s) of the specific designations clearly visible on their business cards and resumes, much in the same way an accountant displays CPA or a financial consultant highlights CFA. In the information security world, IDC divides certifications into two categories: vendor neutral and vendor specific. A vendor-neutral certification, such as Certified Information Systems Security Professional or Certified Information Systems Auditor, encompasses a broad scope of knowledge and is not tied to any one specific technology vendor or product. Vendor-specific certifications, such as Cisco Certified Security Professional or Microsoft Certified Systems Engineer:

Security, are offered by technology vendors that cover knowledge and content relevant only to their products, solutions, and best practices. As mentioned previously in the Security Workforce Profile section, information security professionals participating in the survey have achieved multiple certifications. Across all regions, each responding security professional has at least one vendor-neutral certification, with fewer than half possessing one or more vendor-specific certifications. Both types of certification play extremely important roles in the market, each fulfilling specific knowledge and learning requirements of IT security professionals and demonstrating acceptable levels of competency and experience.

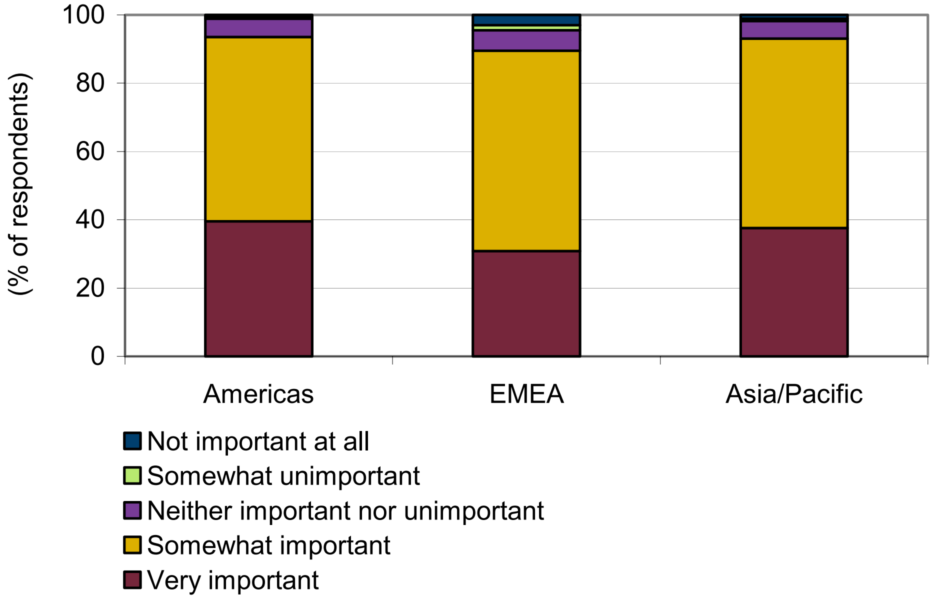
Across all regions, each responding security professional has at least one vendor-neutral certification, with fewer than half possessing one or more vendor-specific certifications.

According to more than 88% of the 1,635 respondents responsible for managing their organization's internal security staff, certifications are considered to be either somewhat or very important during the hiring process (see Figure 14). One of the main attractions leading IT professionals to attain certification status is it affords them the opportunity to differentiate themselves from other candidates with equal or lesser qualifications and potentially increase their salary.

Information security professionals are bullish on the benefits of certification and believe the rewards will lead to challenging and satisfying careers. Independent of geographic location, security practitioners thought information security certifications would enable to them have fruitful security careers, as shown in Figure 15. Sentiment regarding their chances for personal career growth with certification(s) in hand in the Americas and AP was slightly more positive than for those in EMEA.

FIGURE 14

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

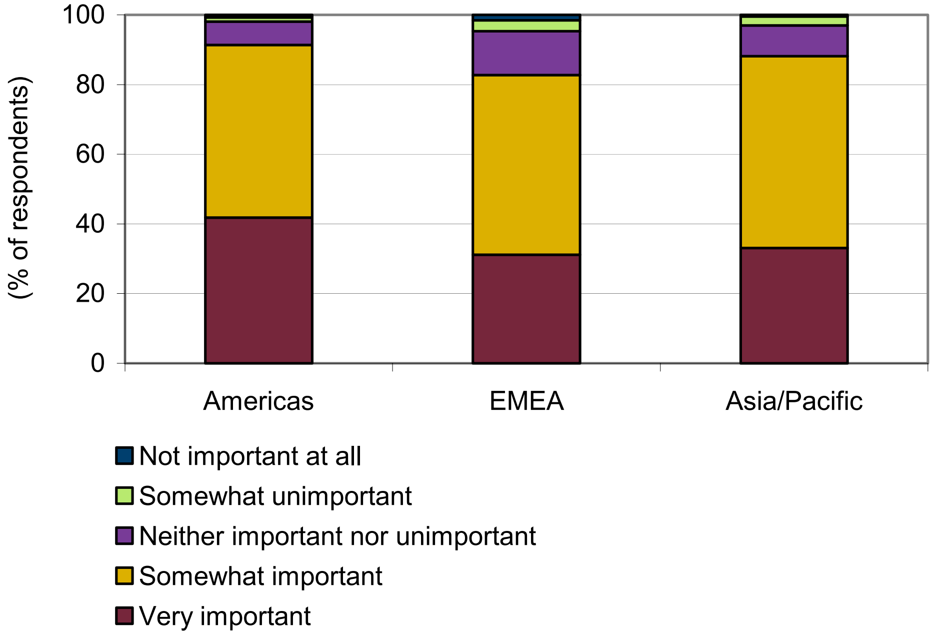


n = 2,133

Source: IDC's *Information Security Global Workforce Survey,* 2004

FIGURE 15

Importance of Information Security Certifications to Information Security Professionals' Career Growth by Region



n = 5,028

Source: IDC's *Information Security Global Workforce Survey,* 2004

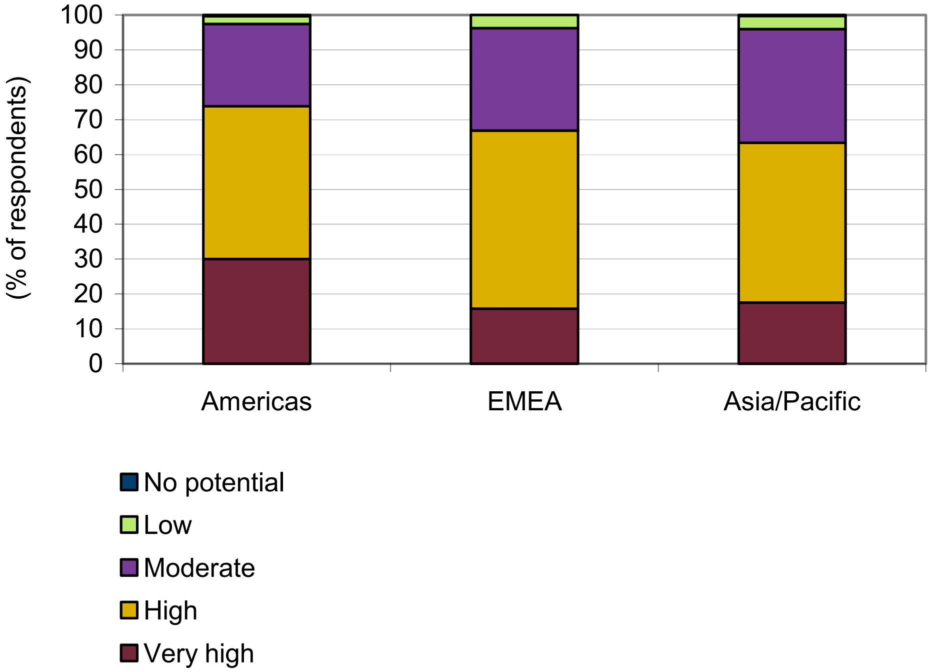
FUTURE OUTLOOK

IT and information security professionals have reason to be positive about the future of their profession and their careers.

Economic indicators are signaling stability in the marketplace. Corporate earnings have been in line with analyst expectations, executive management are talking about increasing corporate investments in the areas of technology refresh and capital expenditures, the forecast for increased staffing looks positive, and corporate profits will continue to support a meaningful IT recovery. The global economic recovery is steadily improving, touching upon every major region of the world. Therefore, IT and information security professionals have reason to be positive about the future of their profession and their careers. In general, this group tends to be cautiously optimistic as a result of the roller-coaster ride of world events, such as the burst of the dot-com bubble, 9/11 and the resulting war on terrorism, and high-profile corporate accounting scandals. Despite these events, security professionals have endured, although those in the Americas and EMEA are more optimistic about their potential for career growth than their colleagues in AP (see Figure 16). At the very least, they believe the job market, in particular their careers and opportunities within the information security industry, will reasonably improve for the foreseeable future.

FIGURE 16

Information Security Professionals' Expectations for Career Growth by Region



n = 5,039

Source: IDC's *Information Security Global Workforce Survey,* 2004

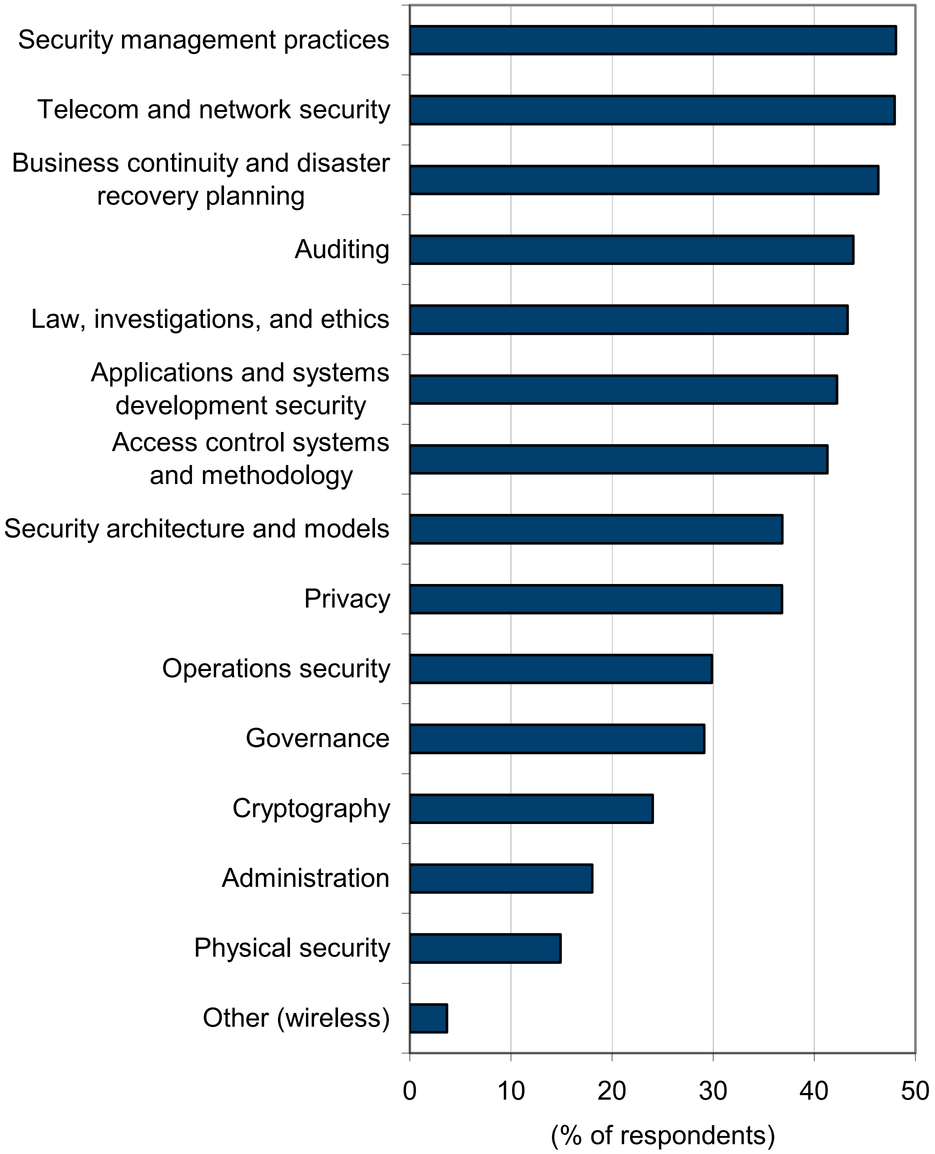
Many higher education institutions worldwide have made significant investments in staff and curriculum to develop concentrated degrees and certificates at both the undergraduate and graduate levels.

As discussed previously, many security professionals have achieved some level of higher education. To ensure continued momentum of the information security profession and because the academic community also believes the growth potential for information security is high, information assurance programs abound. Many higher education institutions worldwide have made significant investments in staff and curriculum to develop concentrated degrees and certificates at both the undergraduate and graduate levels. The original group of 7 in the U.S. Centers of Academic Excellence in Information Assurance Education (CAEIAE) program has expanded to more than 55, with at least 1 center in 27 of the 50 states across the United States. Under this program, four-year colleges and graduate-level universities are eligible to apply to National Security Agency (NSA) to be designated as CAEIAE. Each institution must pass a rigorous review and demonstrate its commitment to academic excellence in information assurance education. This designation only lasts for three years, after which time institutions must reapply.

Throughout the spectrum of security topics, a few of the key areas where information security professionals see an unmet need for additional training and certification include security management practices, telecommunications and network security, and business continuity and disaster recovery planning, as illustrated in Figure 17.

FIGURE 17

Next Frontiers for Information Security Training and Certification



n = 5,020

Note: Multiple responses were allowed.

Source: IDC's *Information Security Global Workforce Survey,* 2004

For information security professionals who wish to rise up through the ranks of management to executive status, knowledge of management best practices and business-related skill sets are crucial to successful career progression. Not only are IT skills and knowledge important, but they must be augmented with solid business understanding of policy, processes, and personnel for information security professionals to obtain the title of chief security officer or equivalent.

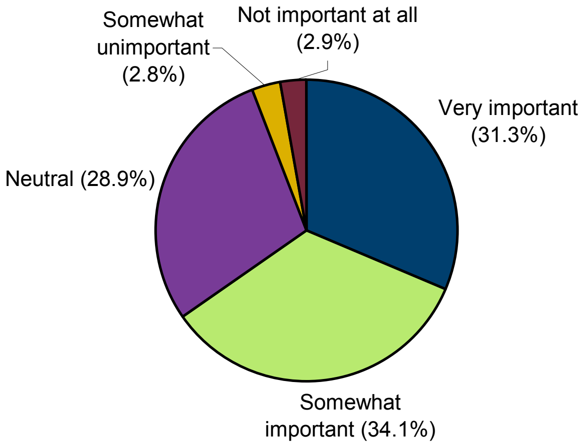
Another factor that will impact the information security of an organization is the emergence of IP telephony or voice over IP (VoIP). This technology transcends two traditionally separate systems (voice and data) and managing groups to bring the promise of a converged network. The resulting new security vulnerabilities and mitigating technologies must be understood and employed to ensure availability, reliability, and security of operations. In addition, VoIP, business continuity, and disaster recovery have been elevated to top of mind. The challenge has become leveraging best practices and solutions to cost-effectively and efficiently ensure the resumption of business in a timely manner. Respondents also noted an additional need for specialized security training and certification in legal and ethics, application security, and wireless technologies.

For providers of information security certifications looking for areas to address and expand into new markets, one method for improving the information security certification process is to evaluate the applicability of new standards as they become internationally recognized. This standardization promotes mobility and cross-pollenization of the information security workforce. The newly created ISO/IEC 17024 standardizes the certification process that provides a uniform set of guidelines for organizations managing the qualifications and certification of individuals, including procedures for the development and maintenance of a certification scheme. Members of the information security community feel that their information security certifications should be accredited under the new ISO standard accreditation. Figure 18 exemplifies the global concern of more than 60% of the survey's respondents for meeting ISO accreditation.

The newly created ISO/IEC 17024 standardizes the certification process that provides a uniform set of guidelines for organizations managing the qualifications and certification of individuals.

FIGURE 18

Importance of Information Security Certification Accreditation Under ISO/IEC 17024



n = 5,040

Source: IDC's *Information Security Global Workforce Survey,* 2004

ESSENTIAL GUIDANCE

Given the sentiments of information security professionals around the world, it is difficult not to be positive about the outlook for this group. Based on the results of this survey and other industry research conducted by IDC, we share in the information security professionals' enthusiasm for what the future may hold. History has proven the path to the future is not always smooth and its course impossible to chart. Knowing these things, however, information security professionals should keep in mind the following constants as they assess their careers:

- Certifications will always be a differentiating factor in the hiring process, so invest wisely. They will certainly open doors and act as a solid foundation for career development.

Certifications will always be a differentiating factor in the hiring process, so invest wisely.

- Augment your technical skill sets and capabilities with business acumen to become a more rounded information security practitioner. Progression up the organizational chain requires business knowledge, which will become an invaluable asset in your toolkit.
- Stay on the leading edge of technology adoption curves to be well-positioned to understand their associated risks to your organization. We spend so much time among the trees that it becomes difficult to visualize the forest.

Copyright Notice