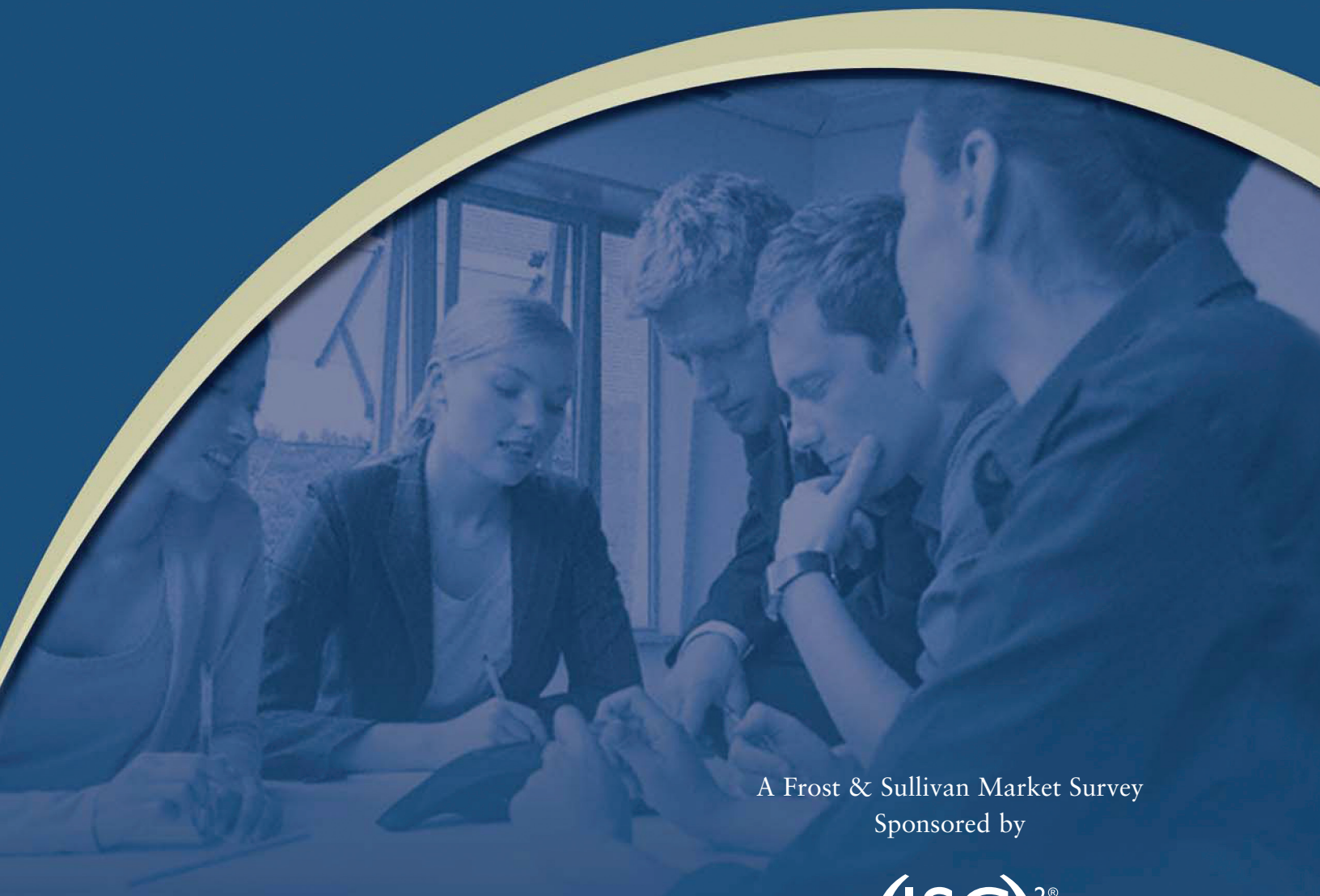
FROST & SULLIVAN

The 2011 (ISC)² Global Information Security Workforce Study



A Frost & Sullivan Market Survey
Sponsored by

(ISC)²®

and Prepared by

Robert Ayoub, CISSP
Global Program Director, Information Security

TABLE OF CONTENTS

EXECUTIVE SUMMARY

On behalf of (ISC)[2®], Frost & Sullivan was engaged to provide detailed insight into the important trends and opportunities emerging in the information security profession worldwide. The electronic survey was conducted through a Web-based portal, where 10,413 information security professionals from companies and public sector organizations around the globe offered their opinions about the information security profession. Topics covered in the survey range from the years of experience in information security and training received to the value of certifications and the most critical threats to organizations today.

As a result of this year's survey, Frost & Sullivan sees the information security professional under increasing pressure to provide even more services to the organization to protect not just the organization's systems and data, but also its reputation, its end-users, and its customers.

Frost & Sullivan believes this year's survey shows a clear gap in skills needed to protect organizations in the near future. The information security community admits it needs better training in a variety of new technology areas, yet at the same time reports in significant numbers that these same technologies are already being deployed without security in mind. The profession as a whole appears to be resistant to adopt new trends in technology, such as social media and cloud computing, which are widely adopted by businesses and the average end-user. The information security profession could be on a dangerous course, where information security professionals are engulfed in their current job duties and responsibilities, leaving them ill-prepared for the major changes ahead, and potentially endangering the organizations they secure.

This is not to say the industry is doomed. If the projected growth in number of information security professionals and concurrent increases in training continue, these risks can be reduced.

Some key findings of this year's study include:

- **Application vulnerabilities represent the number one threat to organizations**. More than 20 percent of information security professionals reported involvement in software development.
- **Mobile devices were the second highest security concern for the organization,** despite an overwhelming number of professionals having policies and tools in place to defend against mobile threats.
- **Professionals aren't ready for social media threats**. Respondents reported inconsistent policies and protection for end-users visiting social media sites, and just less than 30 percent of respondents had no limits set whatsoever.
- **A clear skills gap exists that jeopardizes professionals' ability to protect organizations in the near future**. This year's survey repeatedly illustrates the deployment of new technologies in the enterprise being offset by a demand for more security education on these technologies.

- **Information security professionals weathered the economic recession very well**. Three out of five respondents reported receiving a salary increase in 2010. Overall, salaries for information security professionals increased, with the Asia-Pacific (APAC) region showing the highest growth at 18 percent since the 2007 study.

- **Cloud computing illustrates a serious gap between technology implementation and the skills necessary to provide security**. More than 50 percent of information security professionals reported having private clouds in place, and more than 40 percent of respondents reported using software as a service, but more than 70 percent of professionals reported the need for new skills to properly secure cloud-based technologies.

- **Developing countries illustrated opportunities for growth with an experienced and more educated workforce**. On average, survey respondents in developing countries only had two fewer years of experience than their developed counterparts. They also spent more time on security management and less time on internal issues than their developed country counterparts.

- **The information security workforce continues to show signs of strong growth**. As of 2010, Frost & Sullivan estimates that there are 2.28 million information security professionals worldwide. This figure is expected to increase to nearly 4.2 million by 2015.

Even as the skills gap is becoming urgent, Frost & Sullivan is encouraged by many of the findings of this survey. Management support and end-user training have been embraced by many organizations. Budgets and spending are expected to increase in the next 12 months, and salaries showed healthy growth despite a global recession.

METHODOLOGY

The 2011 Global Information Security Workforce Study (GISWS) was conducted during the fall of 2010 on behalf of (ISC)^2, a not-for-profit organization dedicated to providing education, certification, and peer-networking opportunities for information security professionals throughout their careers. The objective of this study is to provide meaningful research about the information security profession to industry stakeholders, including professionals, corporations, government agencies, academia, and other interested parties, such as hiring managers. The electronic survey portion of this study was conducted via a Web-based portal, with traffic driven to the site using e-mail solicitations.

Frost & Sullivan surveyed 10,413 information security professionals from companies and public sector organizations around the globe to gather their opinions about the information security profession. Seventy-two percent were (ISC)^2 members, while the remaining were non-members. The few occasions where their answers differed significantly are noted in the report. The average experience of respondents worldwide was more than nine years, while five percent of respondents held executive titles such as Chief Information Security Officer. Additionally, Frost & Sullivan 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:

- Employment in the information security profession;
- 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.

This year's survey represents the largest number of respondents to this survey. More countries are represented than ever before, and the average number of years of experience in industry is higher than in previous surveys. This allows Frost & Sullivan to provide an authoritative industry view that is representative of the global industry workforce at large.

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

INTRODUCTION

Recent headlines illustrate the severity of the threat to data. From last year's attacks on Google China, to top-secret communications leaked through WikiLeaks, no data or organization is sacred or safe from attack. The challenge of controlling data is monumental, and the past year has illustrated the tip of the iceberg for data mobility. For example, Apple's iPad sold 3 million units in its first 80 days and was expected to more than double that number by the end of 2010.[1] Google's Android platform also made a remarkable splash in the market. Frost & Sullivan's research shows that smartphones are growing at a rate of 21 percent in North America alone, and the newest devices—tablets and e-readers—are expected to be the next devices of choice, with an expected 22 million units sold in North America by 2016.[2]

The role of the information security professional has been steadily changing during the past decade. They are now responsible for the security of many facets of an organization, including regulatory compliance, human resource and legal compliance, data security, and access control, to name a few. As a result of the increased nature of such a position, information security professionals weathered the economic recession better than other professionals in other industries. In fact, three out of five (ISC)^2 members reported a salary increase within the past year. Frost & Sullivan has identified three key areas of growth in this field:

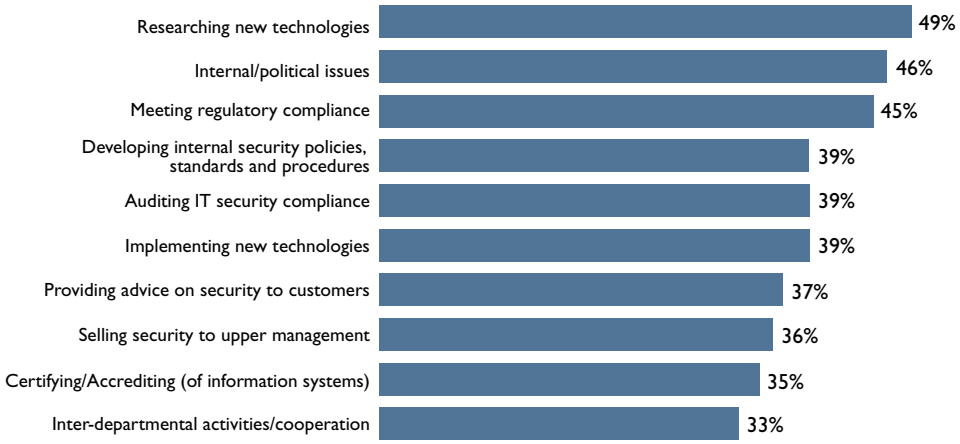
- Regulatory compliance demands (both vertical and geopolitical);
- Greater potential for data loss via mobile devices and mobile workforce;
- Loss of control as organizations shift data to cloud-based services.

This year's study continues to affirm these three growth areas. Figure 1 illustrates the activities that consume a significant portion of an information security professional's time. Little has changed since the 2008 report, as most professionals continue to spend their time fighting internal issues, keeping the organization in compliance, and researching new technologies. One shift from 2008 is the indication that more professionals are spending their time addressing security concerns of customers.

[1] http://www.apple.com/pr/library/2010/06/22ipad.html

[2] 2010 North America eReaders Market

Figure 1—Most Time-Consuming Activities



Frost & Sullivan believes the 2011 GISWS paints a picture of an industry that has matured significantly during the past decade. Information security professionals find their profession being taken seriously by upper management and are being relied upon for the security of the most mission-critical data and systems within an organization. Unfortunately, the 2011 GISWS also shows a marked increase in the technology trends and devices being deployed, and additional responsibilities and pressures being placed upon the information security professional. Frost & Sullivan believes the next several years could show severe gaps in skill sets industry-wide. Information security professionals are stretched thin, and like a series of small leaks in a dam, the current overstretched workforce may show signs of strain.

Demand for Professionals

Frost & Sullivan estimates the number of information security professionals worldwide in 2010 to have been approximately 2.28 million. This figure is expected to increase to almost 4.24 million by 2015, displaying a Compound Annual Growth Rate (CAGR) of 13.2 percent from 2010 to 2015 (see Table 1 below). The Asia-Pacific (APAC) and Europe, Middle East, and Africa (EMEA) regions will present strong growth opportunities for these professionals as well.

Historically, APAC and EMEA regions have lagged behind the Americas region by approximately 12–18 months in deployment and adoption of information security solutions. As the concerns over data loss have become global, this gap has decreased, and the major global regions are set to experience healthy growth rates along with the Americas. Table 1 reflects these findings from our observations of staffing behavior during the past 12 months and from our primary research on organizations' intentions to increase their information security budgets, including staffing.

Table 1—2010-2015 Forecast for Information Security Professionals[3]

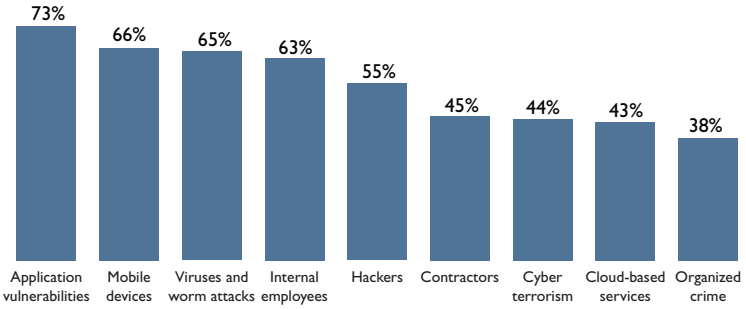
	2010	2011	2012	2013	2014	2015	2010-2015 CAGR
Americas	920,845	1,058,972	1,214,641	1,393,193	1,570,128	1,785,236	**14.2%**
EMEA	617,271	703,689	796,576	897,741	1,014,448	1,148,355	**13.2%**
APAC	748,348	830,666	924,531	1,038,248	1,168,029	1,310,529	**11.9%**
Total	**2,286,464**	**2,593,327**	**2,935,748**	**3,329,183**	**3,752,605**	**4,244,120**	**13.2%**

TECHNOLOGY TRENDS AND CHALLENGES

Since 2008, numerous technology trends have moved into the mainstream. Capturing the trends that have a great impact on information technology is important to measure the effect on the information security profession. The three primary new technology trends studied in detail in 2010 were mobile devices and mobility, cloud computing, and social media.

These new technology areas also represent the greatest risks to organizations. Figure 2 shows the top security threats to organizations in order of severity. Frost & Sullivan believes this illustrates the ubiquity of modern threats.

Figure 2—Top Security Threat Concerns



Mobile Devices and Mobility

The proliferation of mobile devices in the modern organization is staggering. With so many mobile devices in the enterprise, defending corporate data from leaks either intentionally or via loss or theft of a device is challenging. Figure 3 shows the popularity of mobile devices in the enterprise, with 70 percent of respondents indicating that more than 25 percent of their organization has mobile computing devices. Figure 4 illustrates the threat posed by mobile devices. Mobile devices were ranked second on the list of highest concerns by information security professionals, with 66 percent of respondents worldwide reporting mobile devices as a top or high concern.

[3] The forecast presented in this study represents Frost & Sullivan's best estimates and projections for the 2010 - 2015 information security professionals market. These estimates are built using data from a variety of sources, including credible secondary sources, internal research and interviews with professionals in various industry sectors. This estimate includes professionals in a variety of information security roles, both managerial and operational. These estimates include professionals whose job titles specifically indicate information security and those whose primary job function is related to information security activities. 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.

Figure 3—Percentage of Workforce with Mobile Devices by Region

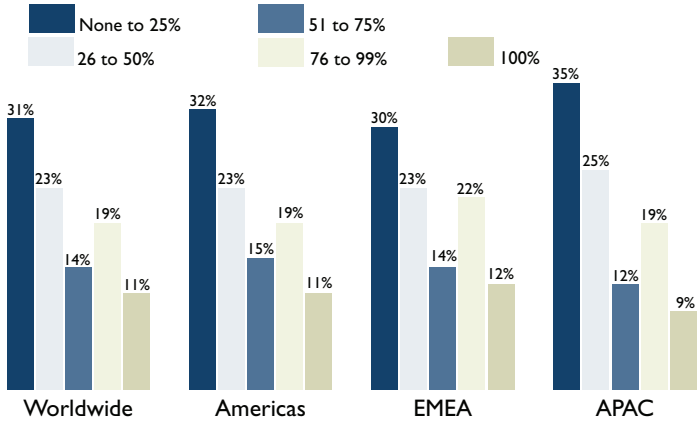
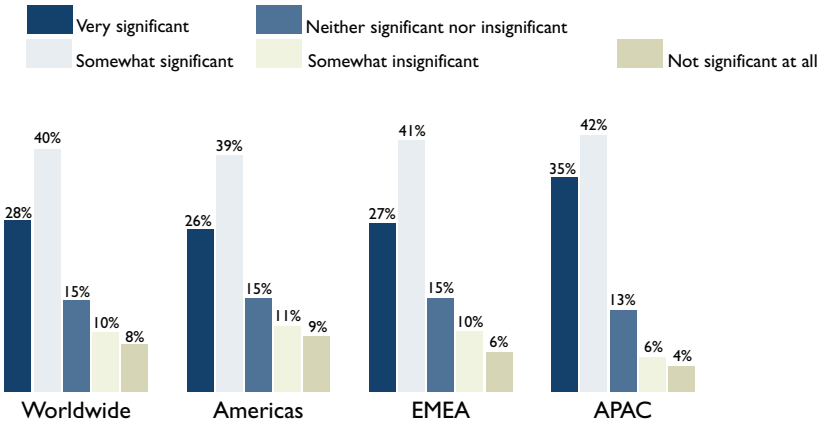
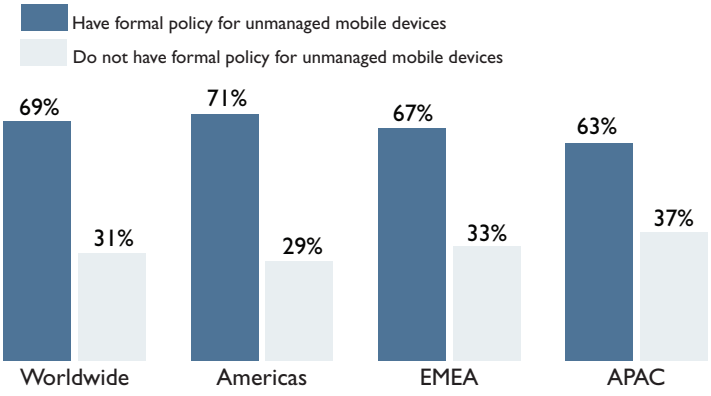


Figure 4—Risks of Mobile Devices by Region



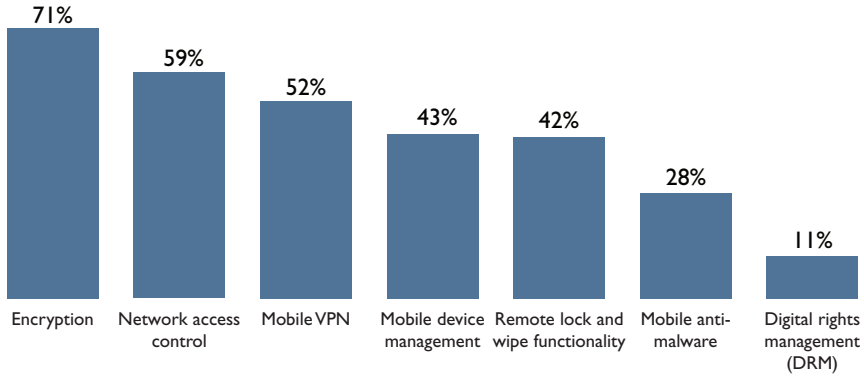
Frost & Sullivan believes the severity of the mobile threat is clearly illustrated by figures 5 and 6. Information security professionals have been tackling the mobile security problem through formal policy and technology. Nearly seven out of 10 respondents worldwide indicated they have a formal policy for mobile devices.

Figure 5—Formal Policy for Unmanaged Mobile Device Use by Region



Information security professionals have also deployed a wide variety of technologies to protect mobile devices. Encryption, Network Access Control (NAC), mobile VPNs, and remote lock-and-wipe functionality are the most popular technologies deployed within organizations. With so many professionals reporting policies in place and technology deployed, while ranking mobile devices as the number two highest concern, Frost & Sullivan believes mobile security could be the single most dangerous threat to organizations for the foreseeable future.

Figure 6—Mobile Device Security Products in Place

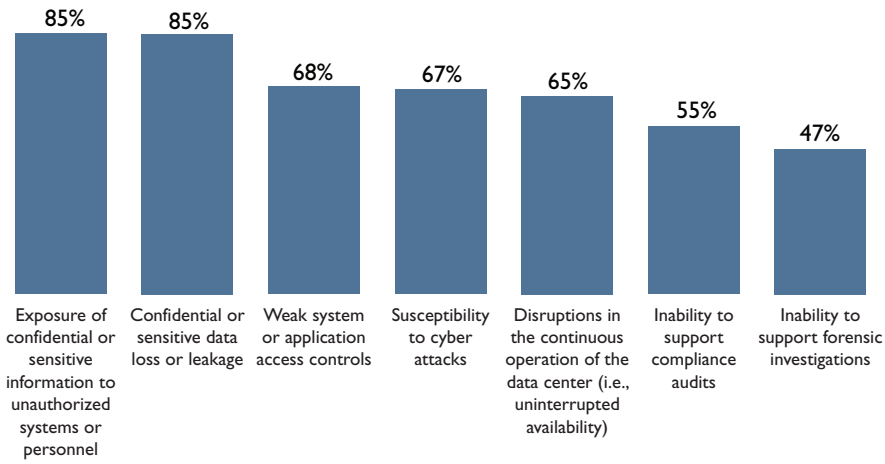


Cloud Computing

Cloud computing is one of the most highly discussed topics in computing today. Organizations see cloud computing as an enabler for more powerful, flexible and scalable computing. However, numerous security concerns arise from the model of cloud computing, with no clear solution to issues such as compliance, data security, and access once the data leaves the host organization. Information security professionals are a key part of the migration to the cloud and have serious concerns about cloud computing.

Respondents believe that the exposure of confidential or sensitive information, data loss, or leaks are of greatest concern to them, with more than half rating this as a top concern. Weak systems, susceptibility to cyber attacks, and disruption in operations ranked much lower (Figure 7).

Figure 7— Security Concerns of Cloud Computing



Compared to other challenges in the industry, cloud computing is one area in particular where information security professionals cited the need for additional training. When asked about the need for new skills for handling cloud computing services, information security professionals overwhelmingly responded that new skills are needed (Figure 8). The skills professionals indicated as necessary for cloud computing are different from traditional security skills. Figure 9 shows a detailed understanding of cloud computing and its associated technologies as highly desired by information security professionals (92 percent and 82 percent worldwide, respectively), followed by a demand for specialized skills in contract negotiation.

Figure 8—Are New Skills Required for Cloud Computing by Region?

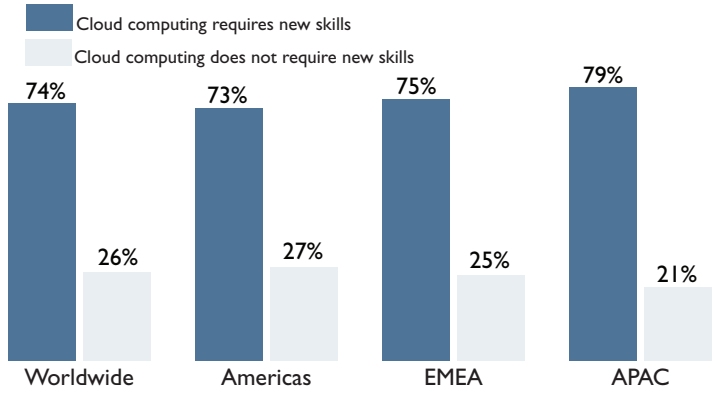
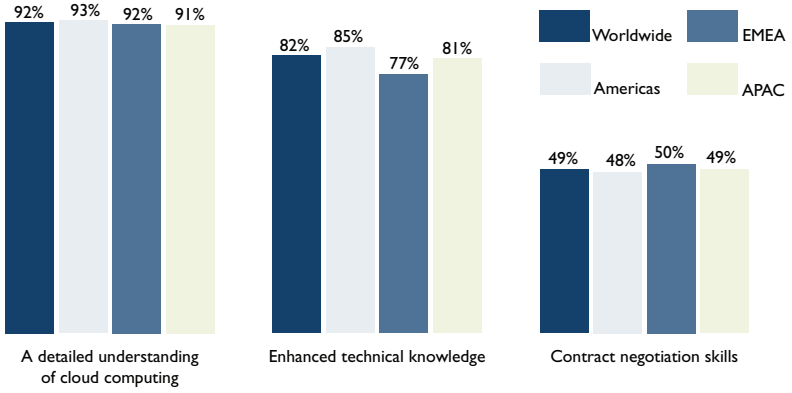


Figure 9—Specific New Skills Required for Cloud Computing by Region



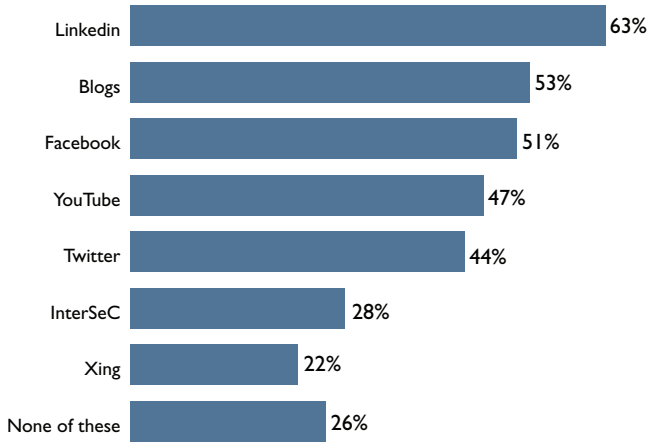
Frost & Sullivan believes the demand of organizations to implement cloud technologies and the indicated requirement of information security professionals for more education shows a significant and potentially dangerous gap between the goals of CIOs and the security required for these services.

Social Media

The explosion and impact of social media since 2008 is obvious. From its beginnings as "fun" platforms such as Friendster and MySpace to the current incarnations of Facebook, LinkedIn, and Twitter, social media is being tapped as a business tool in addition to a

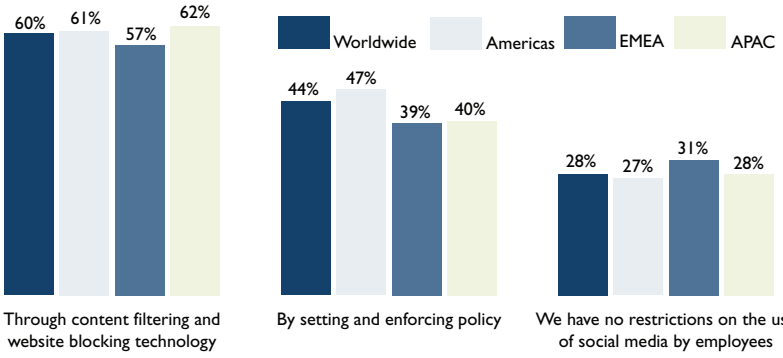
personal tool. Organizations are using social media to connect directly with customers, track comments about their products and services, and provide users with unique offerings. Given the increased legitimate business use of social media, security of organizational users on social media sites is paramount. Unfortunately, many information security professionals still appear to believe that social media is a personal platform and are doing little to manage the threats associated with it. Figure 10 shows the percentage of various social media sites that organizations allow end-users to access.

Figure 10—Social Media Sites that End-Users are Allowed to Access in Their Organizations



Frost & Sullivan was disappointed to see that 28 percent of information security professionals worldwide reported having no organizational restrictions on the use of social media. EMEA was even higher, with 31 percent of respondents reporting they had no restrictions on the use of social media (Figure 11).

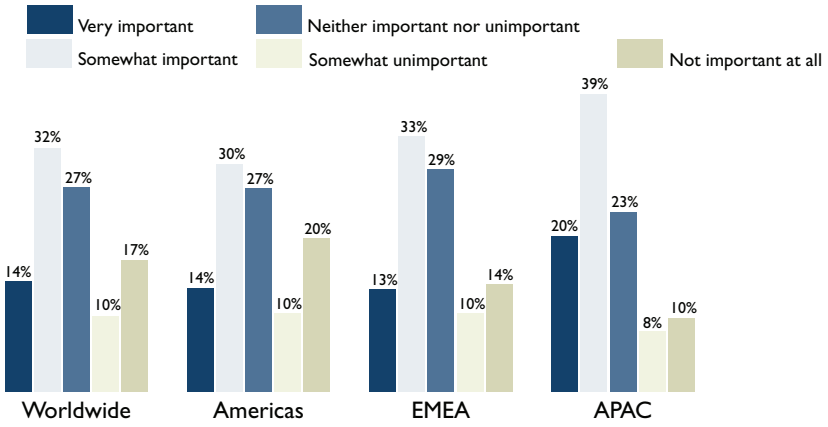
Figure 11—Access Control Methods for Social Media Sites by Region



Part of the disconnect between the desire of users to bring their social media into the workplace and the mixed security placed on social media sites might be explained by the attitude of professionals toward social media in their own careers. Worldwide, almost

20 percent of information security professionals reported that social media tools were not important to them (Figure 12). Frost & Sullivan believes numerous reasons exist for the disconnect, including concerns over privacy and security. However, Frost & Sullivan believes that, ultimately, information security professionals will be forced to embrace social media, if only to understand and protect their users from the risks.

Figure 12—Importance of Social Media Tools by Region



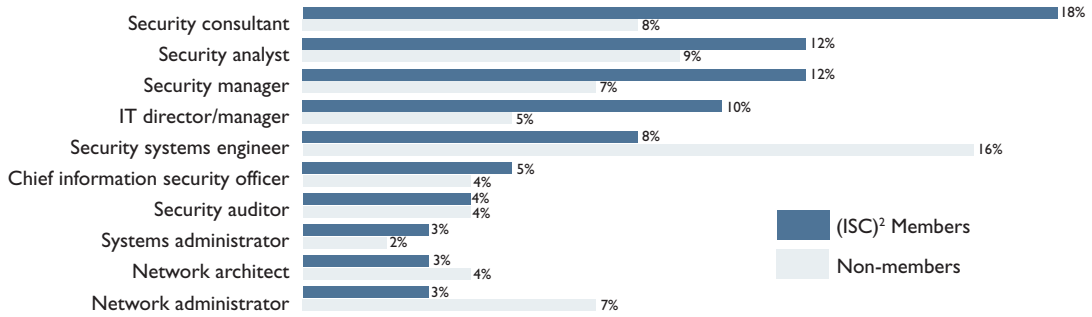
PROFILES OF INFORMATION SECURITY PROFESSIONALS

This year's study reached a broad cross-section of information security professionals in more than 120 countries. Respondents came from the three major regions of the world: the Americas (65 percent), EMEA (23 percent), and APAC (12 percent). Broken down further, Frost & Sullivan found less than one in 10 respondents (8 percent) are from Africa, the Middle East, Latin America, and Oceania. These areas are likely candidates for future growth in information security.

Employment Information

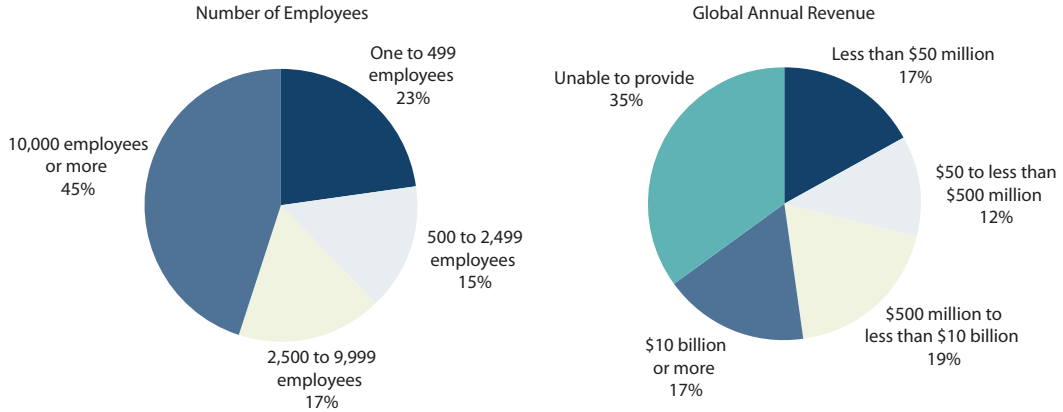
Security professionals who participated in the survey spanned a multitude of job functions and titles, ranging from security analyst to Chief Security Officer (CSO). Figure 13 shows that the highest percentage of (ISC)^2 member respondents (15 percent) were security consultants. Another 11 percent of (ISC)^2 members identified themselves as security analysts. The next most popular response was security managers; and the remaining respondents had a variety of security-related positions, be it security engineer, security manager, or some position whose function was solely related to the information security function of the organization. Each respondent is involved, in some capacity, in information security decisions—ranging from technology selection and security management to hiring staff. Individuals with sole responsibility for physical security were not included in this study.

Figure 13—Respondents by Job Title



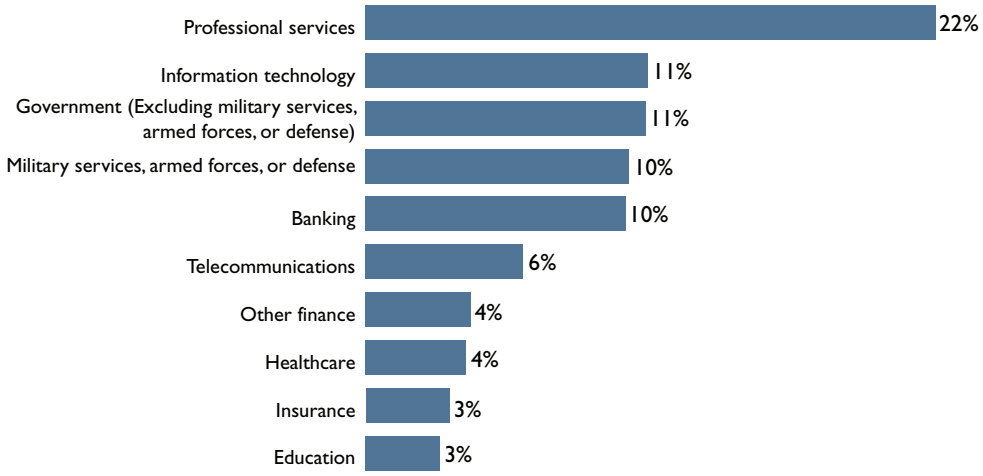
Information security professionals in the 2011 GISWS represent organizations of all sizes. Small organizations (one to 499 employees) accounted for just more than one-fifth of total respondents. Organizations with more than 500 but less than 10,000 employees made up more than one-third of respondents, and companies with more than 10,000 employees (see Figure 14) had the most respondents, with just less than 50 percent. Annual revenue was another criterion measured to gain a different perspective on the types of organizations employing information security professionals. Organizations with $50 million in revenues or less employ 17 percent of total respondents. Those organizations generating more than $10 billion in annual revenues employed 17 percent of total respondents.

Figure 14—Respondents by Company Size and Company Annual Revenue



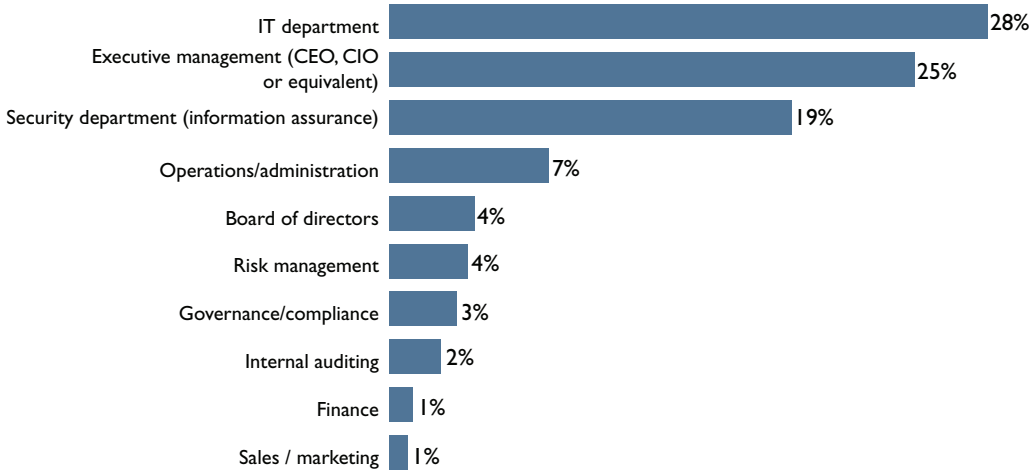
From a vertical perspective, professional services, information technology and governments accounted for the top three industries employing information security professionals (see Figure 15). Regulatory mandates and varying access to resources such as capital and staff force each industry and size of organization to address its information security needs with the right balance of risk versus cost. This balance is continually becoming more challenging to maintain as the need for security permeates more aspects of an organization's operations.

Figure 15—Respondents by Verticals



Reporting lines for the majority of information security professionals worldwide have not changed dramatically during the course of the past 12 months (see Figure 16). Nearly one-third of survey participants responded that they report directly to the IT department, which is slightly less than the 32 percent reported in 2008. Other groups such as risk management, internal auditing, and governance/compliance have become more established in organizational hierarchies during the past two years given the escalating regulatory environment globally.

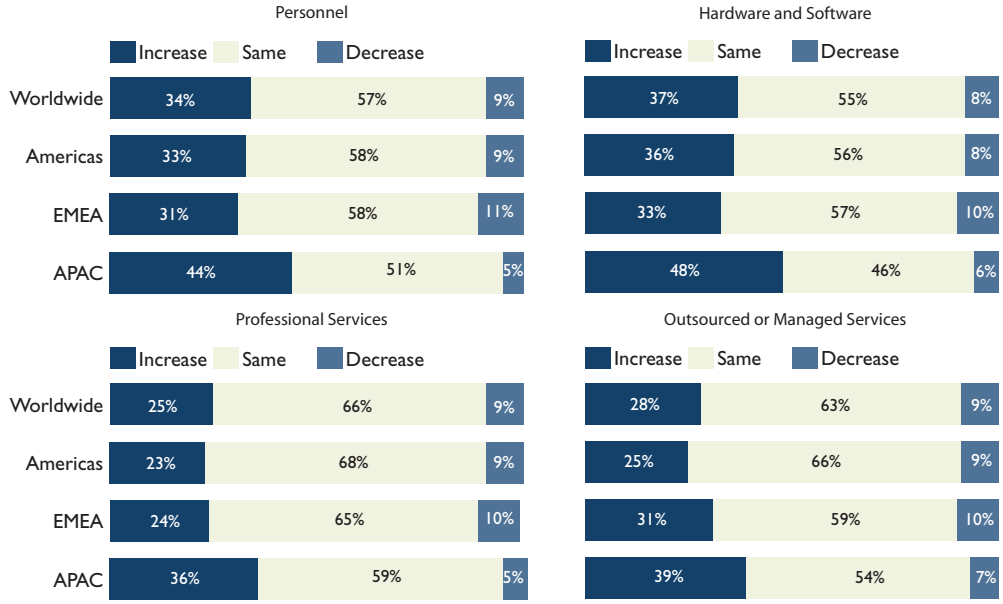
Figure 16—Functional Areas to Whom Information Security Professionals Report



Spending Trends

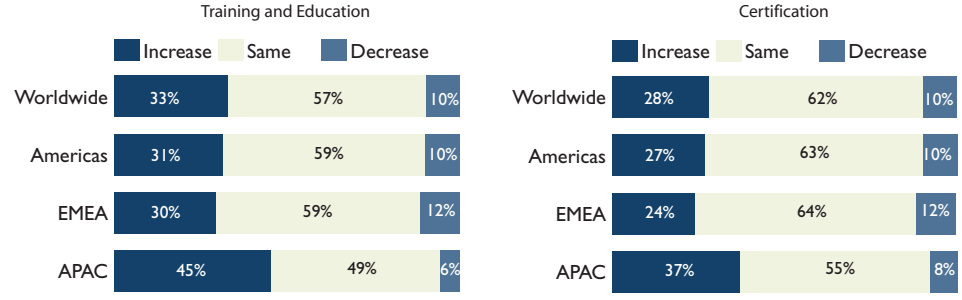
Overall, information security spending on personnel has remained stable in the Americas and EMEA regions in 2011 compared to 2008. In 2008, APAC reported overall higher spending than the rest of the world, and in 2011, this appears to be the case as well. This number includes all expenses to attract, hire, and retain qualified security professionals required to execute an organization's security strategy and achieve its business objectives. In addition, any internal and external security-related training delivered to employees is captured. Figure 17 highlights regional differences in funding a variety of security functions. Since 2007, APAC respondents reported higher than expected increases in personnel, hardware and software, professional services, and outsourced or managed services.

Figure 17—Changes in Information Security Spending



Looking ahead, practitioners are optimistic about increases in budgets for training (see Figure 18) and certification.

Figure 18—Changes in Information Security Training and Certification Spending

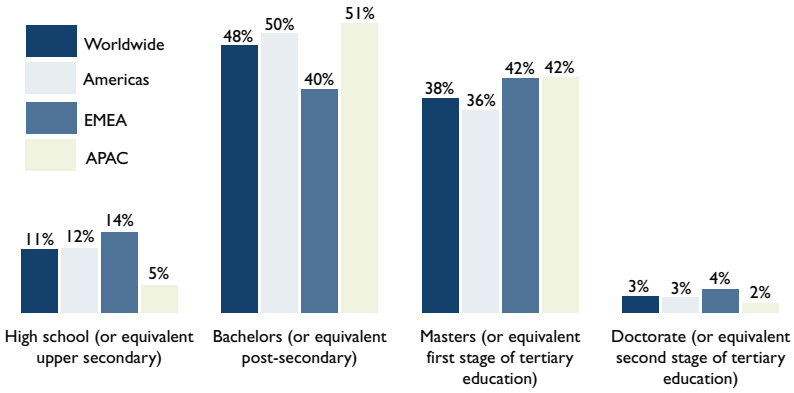


These optimistic results validate what Frost & Sullivan has seen in other research, namely that security continues to be important, not just for the largest organizations, but for organizations of all sizes. Additionally, most organizations are beginning to recognize security as a specialized skill requiring additional, continual training.

Education

From a professional development viewpoint, respondents again reported achieving a high level of education (see Figure 19). More individuals with at least a bachelor's degree or equivalent are employed in the information security workforce. Worldwide, 48 percent of information security professionals have a bachelor's degree, with the Americas and APAC having the highest number, at 50 percent and 51 percent, respectively. EMEA reported the highest number of professionals who hold doctorate degrees, with APAC and the Americas both showing a strong number of respondents having master's and doctorate degrees.

Figure 19—Education Level by Region

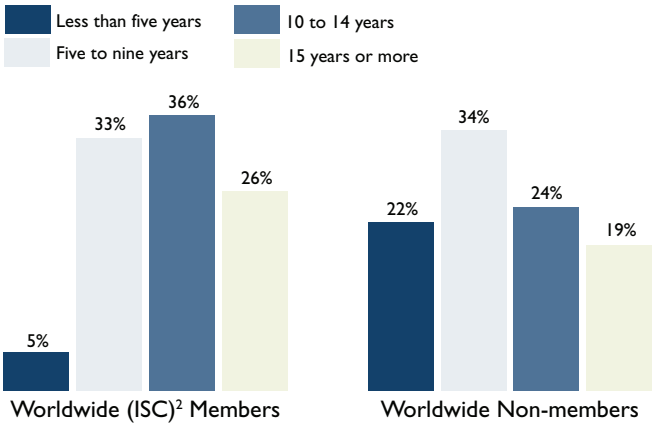


Years of Experience

Years of professional experience proved to be another important candidate criterion considered by hiring managers and their organizations as a complement to, or substitute for, education. With a maturing workforce and new entrants fulfilling staffing needs, some shifts have occurred across reported experience segments. In 2007, security professionals in the Americas averaged 9.5 years of experience, while security professionals in EMEA and APAC averaged 8.3 years and 7.1 years, respectively. This average has gone up, and in 2011, information security professionals averaged 10 years of experience in the Americas and EMEA, and nine years in APAC.

In the Americas, practitioners have the most experience with security. The increasing numbers in these regions show that information security professionals are staying in their roles.

Figure 20—Experience Level by Region



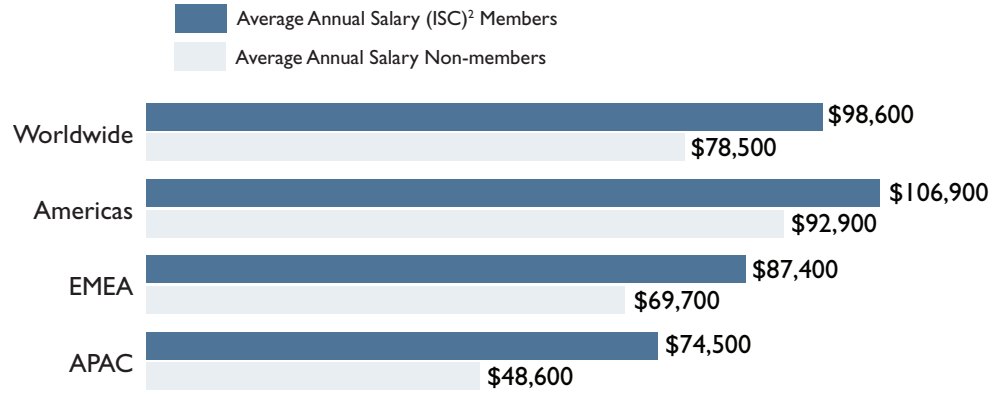
Salary Information

With more individuals achieving higher education levels and gaining valuable experience, information security salaries in 2011 have shifted globally to reflect some of the regional dynamics taking place. In the Americas, the average annual salary for (ISC)² members was $106,900 (compared to $100,967 in 2007). This increase reflects the growing importance being placed on security and the number of experienced professionals in the region. Member salaries in EMEA were also impressive at $87,400.

In previous years, surveys have shown that APAC salaries have lagged significantly; however, the 2011 survey indicates that APAC salaries are becoming more closely aligned to those seen in other regions, moving up to $74,500.

Frost & Sullivan also saw a significant difference in the salaries reported by (ISC)² members compared to information security professionals who do not hold an (ISC)² certification. Even when comparing by years of experience (the majority of (ISC)² members have more than five years of experience), significant differences in salaries appear across the regions.

Figure 21—(ISC)² Member vs. Non-Member Survey Comparison of Average Annual Salary by Region (Five-Plus Years of Experience)



THE CHANGING JOB FUNCTIONS OF INFORMATION SECURITY PROFESSIONALS

The job functions and roles of information security professionals continue to evolve rapidly. Numerous new functional areas are finding their way into the jobs of information security professionals. One of the key new areas of focus is the information security professional's involvement in software development.

Figure 22 shows the industry involvement of information security professionals in software development. Worldwide, 22 percent of respondents indicated they were involved in some aspect of the software development process. They also shared a number of concerns about the risks caused by a variety of development tasks (Figure 23).

Figure 22—Software Development Involvement by Region

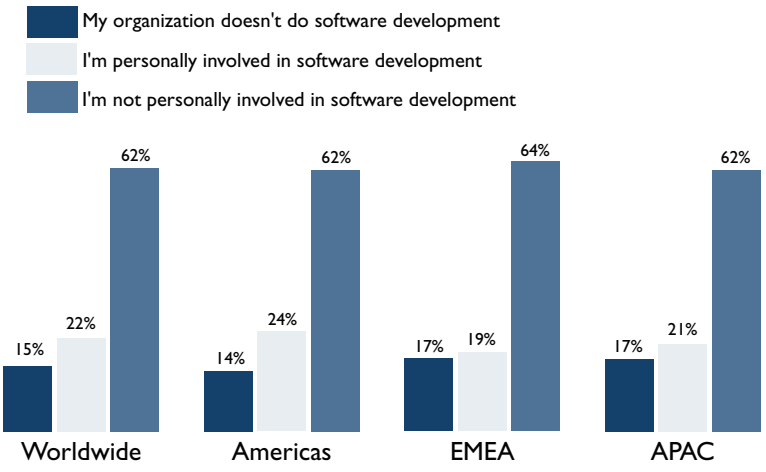
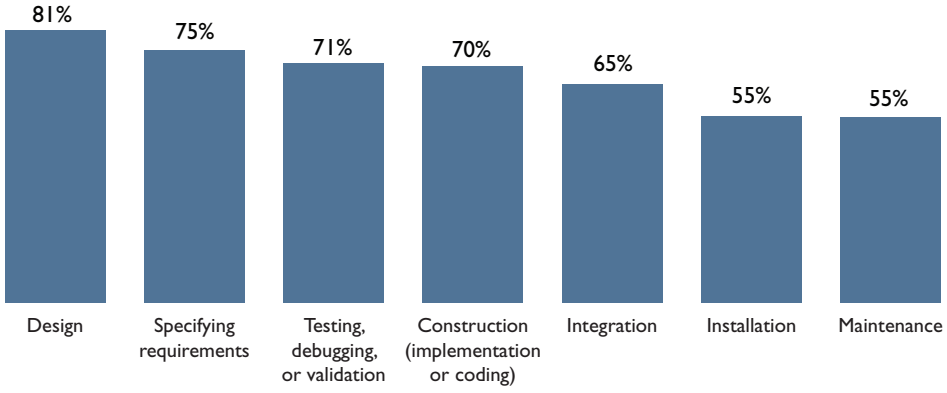


Figure 23—Security Concerns of Software Development



Information Security in Undeveloped Countries

The differences between developed and undeveloped countries provide another indicator of the changing role of the information security professional. While salaries continue to climb in the developed countries, average salaries in developing countries are still relatively low (Figure 24). However, the professionals in undeveloped countries only lag their developed counterparts by two years of experience (10 as opposed to 12 years of experience worldwide) (Figure 25).

Figure 24—Average Salary of Developed vs. Developing Regions

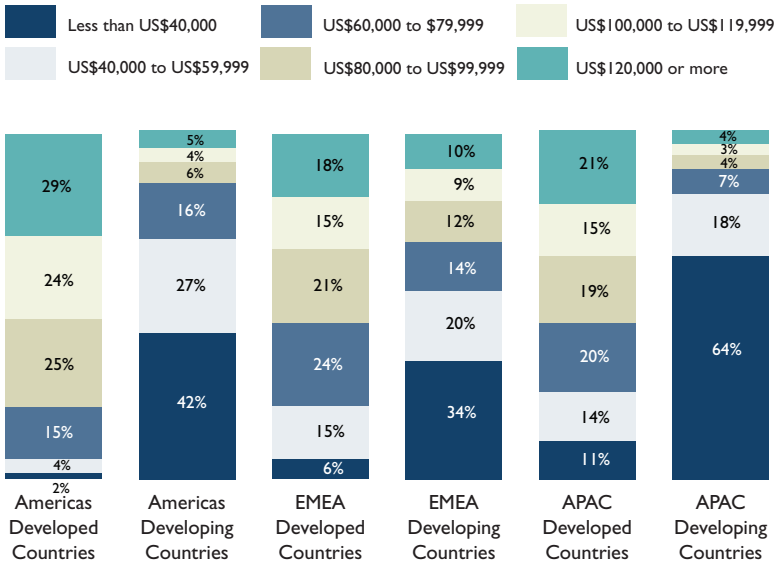
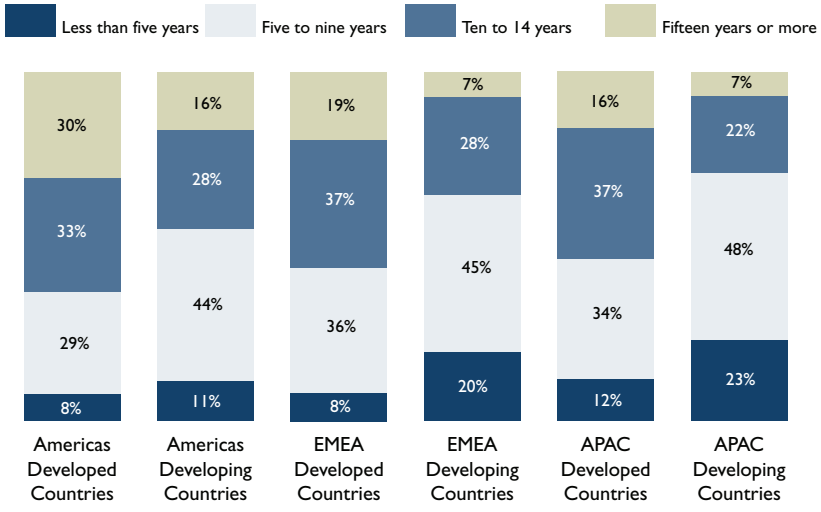


Figure 25—Years of Experience of Developed vs. Developing Regions



It was once considered taboo to outsource any security functions at all. However, as security operations have become more complex, many companies found it was preferable to outsource to a trusted third party in order to keep their data secure. Given the salary difference in developing countries, along with solid experience and skills, developing countries could be a target for security expansion in the future.

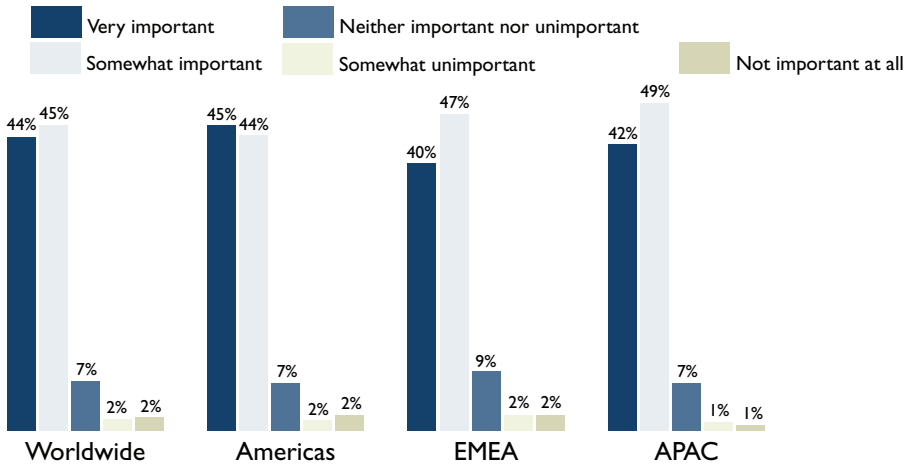
Undoubtedly, the threat landscape will continue to evolve. The constant changes expected in the industry require new skills, not just incremental advances in knowledge. Frost & Sullivan believes that information security professionals will be seeking to develop new skills, not just updates to their existing skills, as new skill sets will be required for professionals to be successful.

WHY INFORMATION SECURITY CERTIFICATIONS REMAIN HIGHLY VALUABLE

Twenty years ago, the skills required to secure a network were learned from experience gained in the military or on the job. It was a new area of IT and not a well-understood discipline. As validation of skills became more necessary, organizations and hiring managers looked to certifications as a means to justify hiring an employee. Attaining a security certification made an important statement to potential employers that an individual had the knowledge, skills, and abilities to defend an organization against possible breaches and build up an organization's defenses. This achievement placed a candidate ahead of the pack, as additional metrics beyond certification were not available.

According to the 74 percent of respondents who were involved in hiring information security staff, the importance of information security certifications as a hiring criterion remains high, with just less than 90 percent of respondents ranking security certifications very or somewhat important (see Figure 26). While certifications are one indication of a better candidate, they do not tell everything about the professional's overall capabilities.

Figure 26—Importance of Security Certifications by Region

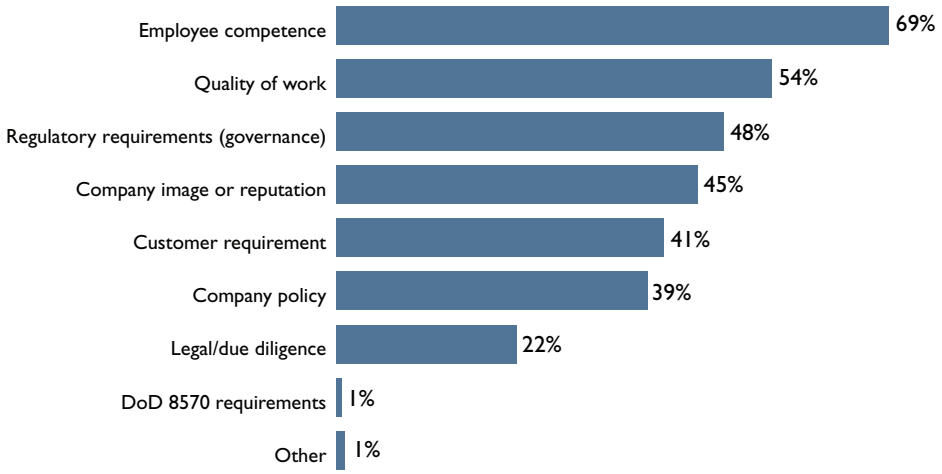


Complexity has been added to the hiring process through the years due to the sheer number and qualitative differences of certifications offered in the marketplace. The list of vendor-neutral and vendor-specific security certifications grows every year, making it difficult for employees, hiring managers, and their organizations to discern which certifications carry the greatest value for them. Today, the number has significantly grown to more than 40 vendor-neutral and vendor-specific certifications. Frost & Sullivan first reported the perception of the dilution effect in the marketplace in the 2008 study. This trend continues to challenge certification vendors to differentiate themselves. The concern is that certifications considered of high value today may be perceived to be devalued and, consequently, less significant to information security professionals and, more importantly, their employers. Frost & Sullivan believes that many vendors are addressing the current skills gap increasing the complexity and continuing education requirements of their certifications.

The onus will shift to the sponsors and providers of both vendor-neutral and vendor-specific security certifications to articulate their value and distinguish themselves from each other. The 2011 GISWS gives some hints into what the future of information security certifications will hold.

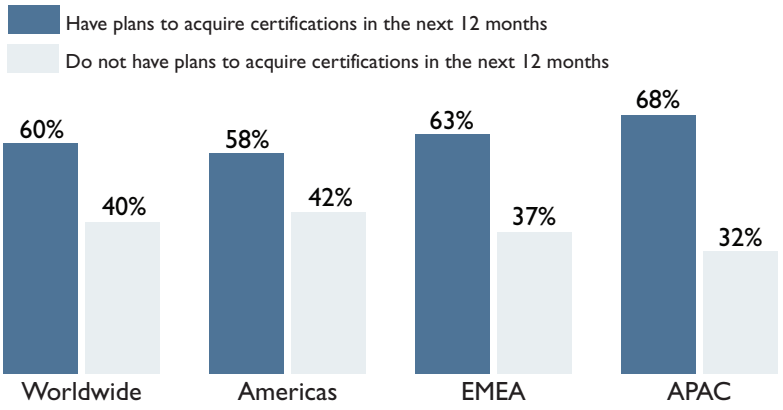
The 2011 GISWS also asked for the top reasons why managers prefer hiring information security professionals with certifications. These are illustrated in Figure 27. Quality of work, company policy, and employee competence remain the major reasons; however, other reasons are surfacing.

Figure 27—Reasons to Hire a Certified Employee



Differentiation from other candidates and potential salary benefits have traditionally been other reasons that individuals interested in information security obtain certifications. Given the recession, Frost & Sullivan believes there is an even greater push by information security professionals to stay relevant. This year's survey confirms this, with six out of 10 respondents reporting they would look for at least one more new certification to add to their toolkits in the 2010–2011 period (see Figure 28).

Figure 28—Plans to Acquire Additional Certifications by Region



Future Training Efforts

In an effort to stay ahead of the curve, information security professionals identified additional training and education opportunities across a number of disciplines. First and foremost was the need for training as it applies to information risk management and applications and systems development security (see Figure 29). Many organizations have come to the realization that their own internally created software suffers from the same security risks as those coming from a vendor.

Figure 29—Growing Need for Training

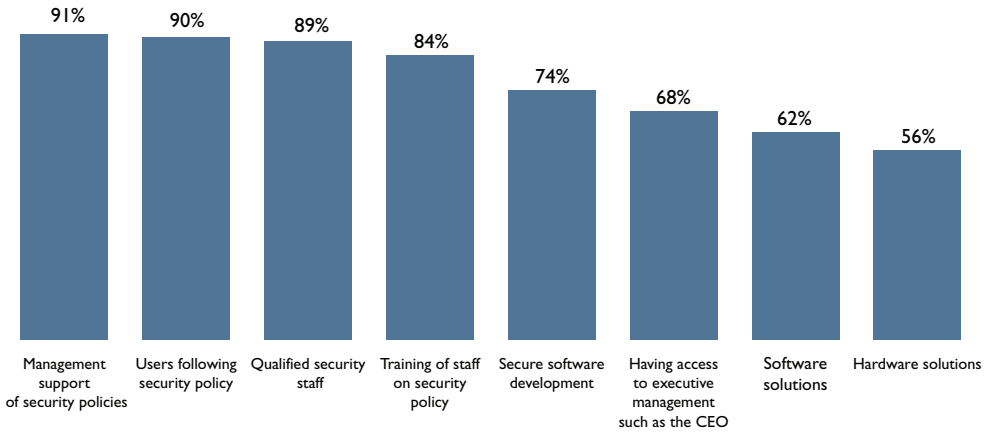
Balancing Openness with Security is Key

Despite an increasing number of roles dedicated to information security, the ultimate responsibility for the security of an organization falls on the shoulders of the end-users. If any one individual fails to maintain and abide by security policies, all the systems and data of the organization are at risk. In the modern organization, end-users' activities and devices are dictating IT and information security departments' priorities. End-users continue to

expect corporate services to operate at the same level that consumer services operate, and many are using personal devices to access the corporate network. This expectation of more open systems (which is why consumer products are so flexible) tends to be at odds with most corporate environments.

Information security professionals remain positive about their ability to influence the organization and have been instrumental in changing the mindset of executives and gaining their buy-in that security is an enterprise-wide problem, not just an IT issue. Information security professionals realize that end-users are a key part of keeping systems secure, and combined with upper management support, information security professionals can keep their organizations open and secure (see Figure 30).

Figure 30—Important Requirements Needed to Secure the Organization



Even since the 2008 study, the importance of *people* in solving many of the challenges today continues to grow. In 2011, six of the top eight organization security concerns are related to the training and enforcement of user policies.

CONCLUSION

2011 looks to be an exciting year for information security professionals. Along with a number of high-profile attacks that have again raised the criticality of the information security profession, many companies are emerging from the global recession ready to hire additional resources and spend money on training and equipment. Security management will always require the proper balance between people, policies, processes, and technology to effectively mitigate the risks associated with today's digitally connected business environment.

Frost & Sullivan believes that the 10,413 information security professionals who shared their views and opinions in this study represent the frontline troops within their organizations. As a result of the 2011 GISWS, Frost & Sullivan advises information security professionals to consider the following conclusions:

- Consumerization has end-users bringing technology to the enterprise instead of the opposite; information security professionals should work to securely embrace these new technologies instead of acting as roadblocks.
- Cloud computing and software development are areas of information security that require new skills, not just incremental advances.
- Compliance is driving organizational behavior from changes in spending levels to shifts in accountability, to requirements in new skill sets.
- As emerging sub-markets, Latin America, Africa, and Oceania offer attractive employment incentives and opportunities for information security professionals over the next five years.
- Certifications will continue to be an important differentiator as the number of professionals necessary to effectively secure organizations continues to increase.

(ISC)² would like to acknowledge and thank the following organizations for their participation in the 2011 (ISC)² Global Information Security Workforce Study: ASIS International, the Association of Information Security Professionals (AISP)—Singapore, Ekelöw Infosecurity, Information Security Solutions, Information Systems Security Association (ISSA) UK, Professional Information Security Association (PISA), the Security Executive Council (SEC), and ShadowSec.

CONTACT US

Silicon Valley
331 E. Evelyn Ave. Suite 100
Mountain View, CA 94041
Tel 650.475.4500
Fax 650.475.1570

San Antonio
7550 West Interstate 10, Suite 400,
San Antonio, Texas 78229-5616
Tel 210.348.1000
Fax 210.348.1003

London
4, Grosvenor Gardens,
London SWIW ODH,UK
Tel 44(0)20 7730 3438
Fax 44(0)20 7730 3343

877.GoFrost
myfrost@frost.com
http://www.frost.com

Auckland
Bangkok
Beijing
Bengaluru
Bogotá
Buenos Aires
Cape Town
Chennai
Colombo
Delhi / NCR
Dhaka
Dubai
Frankfurt
Hong Kong
Istanbul
Jakarta
Kolkata
Kuala Lumpur
London
Mexico City
Milan
Moscow
Mumbai
Manhattan
Oxford
Paris
Rockville Centre
San Antonio
São Paulo
Seoul
Shanghai
Silicon Valley
Singapore
Sophia Antipolis
Sydney
Taipei
Tel Aviv
Tokyo
Toronto
Warsaw

ABOUT FROST & SULLIVAN

Based in Mountain View, California, Frost & Sullivan is a global leader in strategic growth consulting. This white paper is part of Frost & Sullivan's ongoing strategic research into the information technology industries. Frost & Sullivan regularly publishes strategic analyses of the major markets for products that encompass storage, management, and security of data. Frost & Sullivan also provides custom growth consulting to a variety of national and international companies.