FROST & SULLIVAN

THE 2008 (ISC)^2 GLOBAL INFORMATION SECURITY WORKFORCE STUDY

A Frost & Sullivan White Paper
Sponsored by

(ISC)^2

"We Accelerate Growth"

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. An electronic survey was conducted through a Web-based portal, where 7,548 respondents from companies and public sector organizations around the globe offered their opinions about the information security profession in which they are employed. Topics covered in the survey range from the years of experience in information security, from training received, to the value of certifications and new areas where additional training is required.

Some key findings of this year's study are:

- Respondents came from the three major regions of the world: Americas (41%), Europe, Middle East and Africa (EMEA) (25%), and Asia-Pacific (34%). It is also interesting to note that this year, respondents from Africa, Latin America, and Oceania comprised 17% of the total respondents.

- A third of respondents said their primary functional responsibilities are mostly managerial, with a higher proportion of respondents (48%) reporting that their functional responsibilities will be mostly managerial in the next two to three years.

- Respondents from the Americas see a growing demand for education in security administration (53%), applications and systems development for security (39%) and telecommunications and network security (34%).

- Respondents from EMEA see a growing demand for security administration (40%), business continuity and disaster recovery planning (29%) and privacy (29%).

- Respondents from Asia-Pacific see a growing demand for security administration (54%), applications and systems development for security (36%) and telecommunications and network security (34%).

- Three-quarters of respondents see viruses and worm attacks as a top/high threat. Next in line for concern are hackers and inside employees as potential security threats.

- Three quarters of respondents view the impact of service downtime (73%) and damage to the organization's reputation (71%) as top/high priorities. In addition, customer issues related to privacy violations (70%) and customer identify theft (67%) are a top/high priority.

- Banking/Insurance/Finance sector respondents have a greater concern for all security threats, such as hackers, viruses and other threats compared to other industry segment respondents.

- A higher proportion of Government sector respondents see cyber terrorism (41%) as a top/high concern.

Information security professionals are under increasing pressure to secure not just the perimeter of the organization but all the data and employees that belong to the organization. Between the requirement to implement new technologies and security solutions within more restricted budgets, the necessity for specialized training for information security professionals continues to increase. Whether researching new technologies or implementing information risk management initiatives, information security professionals are being held to even more stringent standards than ever before.

METHODOLOGY

The 2008 Global Information Security Workforce Study (GISWS) was conducted during the fall of 2007 on behalf of (ISC)^2, a not-for-profit organization dedicated to providing education, certification, and peer-networking opportunities for information security professionals worldwide. (ISC)^2 engaged Frost & Sullivan to provide detailed insight into the important trends and opportunities in the profession worldwide. The objective of this study is to provide meaningful research data about the information security profession to industry stakeholders, including professionals, corporations, government agencies, (ISC)^2 members, academia, and other interested parties, such as hiring managers. The electronic survey portion of this study was conducted via a Web-based portal, with traffic driven to the site using email solicitations.

Frost & Sullivan surveyed 7,548 respondents from companies and public sector organizations around the globe to gather their opinions about the information security profession. The Web-based surveys targeted information security profession respondents worldwide. 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

For this year's study, the (ISC)^2 member and non-member samples were compared in relative proportion to the actual population of security professionals worldwide. A weighting strategy was developed and applied to the member and non-member samples. Both the member and the non-member samples were weighted based on the regional population proportions for the Americas, EMEA and Asia-Pacific and weighted based on the relative population proportions of members to non-members.

As a result, the survey data and findings are more representative of the global information security professional population worldwide as compared to previous years' survey results. Caution must be exercised when making comparisons with prior years' data. Since the data is now more representative of the overall global information security workforce, differences in areas such as years in the profession, salary, type, and size of organizations are evident in this year's survey findings.

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

INTRODUCTION

High-profile identity theft and data loss incidents, such as those reported by U.S. retail institution TJX, HM Revenue and Customs in the UK, and the Veteran's Administration in the U.S., underscore the critical importance of security in today's organization. Gone are the days when security at the perimeter was the primary focus of information security. For today's organization, it is essential to protect data both at rest and in transit – inside and outside of the organization. Customers expect their data to be protected and have shown that they will leave organizations that violate their trust. On top of data security, the need to comply with regulatory requirements is also paramount.

There is an increasing number of compliance initiatives that organizations are required to comply with, such as Sarbanes-Oxley (SOX) – a U.S. mandate that applies globally to any company trading on a U.S. exchange, Basel II - covering the European financial services sector, the Payment Card Industry (PCI) Data Security Standard (DSS) - covering credit card transactions globally, HIPAA in the U.S., which refers to the healthcare sector, and an increasing number of country- and industry-specific standards, such as Japan's Financial Instruments and Exchange Law (J-Sox) and The Federal Information Security Management Act (FISMA), which regulates U.S. federal government organizations. Organizations are finding themselves being required to adhere to two or more compliance standards. Each standard has varying requirements, and information security professionals have to be talented enough to deal with this growing trend.

This study shows that people are at the root of effective security (51% say internal employees pose the biggest threat). In the past, many organizations and executives looked to technology to solve many of their security challenges. However, with the increasing visibility of security to the executive management and the threats posed by malicious and accidental acts of internal employees, educated, qualified and experienced information security professionals are viewed as the answer to an organization's security challenges.

With the wide variety of compliance initiatives and attacks today, information security professionals must have the knowledge, skills and ability to properly address these challenges. Frost & Sullivan believes that education of organizations by information security professionals is necessary to ensure that organizations understand both the necessity of hiring properly qualified individuals and the possible consequences of hiring under-qualified professionals.

Even with a slowing in the economy in some sectors, Frost & Sullivan believes information security to be a field of continued strong growth. In particular, Frost & Sullivan believes that three primary factors will contribute to this strong growth:

- **Public Confidence** – A noteworthy shift from prior years, the majority of respondents rated preventing damage to an organization's reputation as their highest priority. Frost & Sullivan believes this to be a growing driver not only in the near term but even as companies meet regulatory compliance initiatives. Organizations are finding that significant costs result from data breaches. Many estimates put the cost of any data breach at $50 - $200 per record lost, and those numbers do not include costs that are difficult to quantify, such as reputation damage.

- **Compliance** – Compliance is a primary driving force behind the growth of the profession. Increasingly, regulatory compliance initiatives place the responsibility of compliance squarely on the shoulders of the executive team. This raises the importance of information security within organizations, leading to a growth in the number of professionals.

- **Return On Investment** (ROI) – One of the primary challenges that hiring managers have faced has been to prove that they are getting a return on their investment. Fines for failing to meet regulatory requirements give managers a more tangible measurement for justifying security spending. This, combined with increases in efficiency gained from additional security tools such as Security Event Information Management (SEIM) and Single Sign On (SSO), are creating an environment in which the value of security can be measured with a positive ROI.

Frost & Sullivan estimates the number of information security professionals worldwide in 2007 to have been approximately 1.66 million. This figure is expected to increase to almost 2.7 million professionals by 2012, displaying a compound annual growth rate (CAGR) of 10% from 2007 to 2012 (see Table 1). The Americas and EMEA regions will present higher growth opportunities for information security professionals than the Asia-Pacific region. However, organizations in both the Asia-Pacific and EMEA regions continue to develop compelling propositions to entice qualified professionals.

Table 1 reflects these findings from our observations of staffing behavior during the previous 12 months and from our primary research on organizations' intentions to increase their information security budgets, including staffing.

Table 1 - Worldwide Information Security Professionals by Region, 2007- 2012[1]

	2007	2008	2009	2010	2011	2012	2007-2012 CAGR
Americas	685,700	749,470	822,918	920,845	1,010,167	1,100,072	10%
Asia-Pacific	570,000	625,290	680,316	736,782	795,724	856,995	8%
EMEA	405,900	471,250	541,466	614,023	680,951	737,470	13%
Total	**1,661,600**	**1,846,010**	**2,044,700**	**2,271,650**	**2,486,842**	**2,694,537**	**10%**

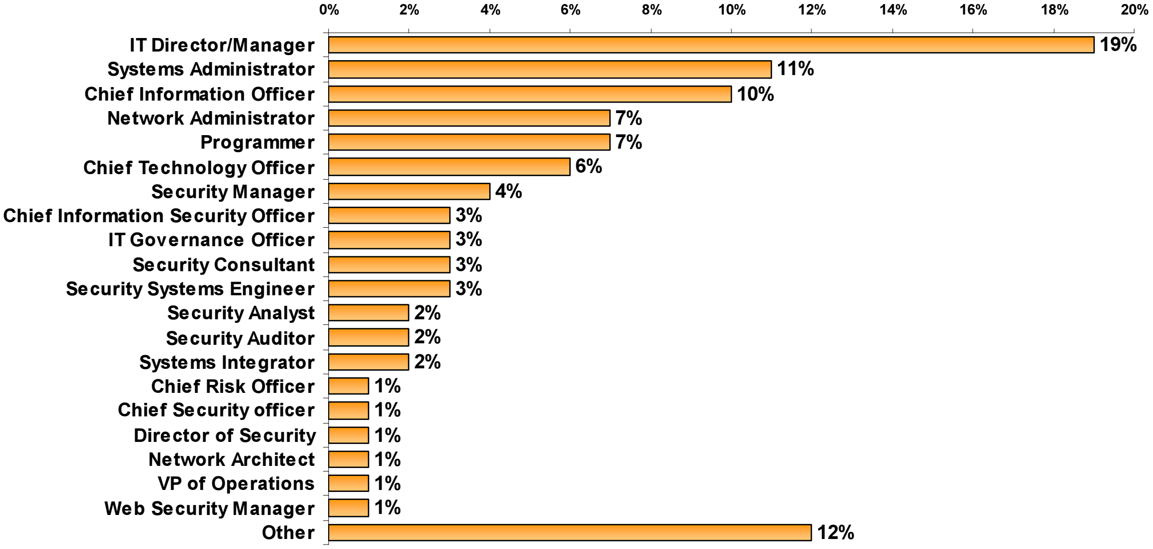
DEMOGRAPHICS

This year's study drew feedback from a broad cross-section of information security professionals in more than 100 countries. Respondents came from the three major regions of the world: Americas (41%), EMEA (25%), and Asia-Pacific (34%). It is also interesting to note that this year respondents from Africa, Latin America, and Oceania (which includes Australia, Fiji, New Zealand, French Polynesia, and Guam) comprised 17% of the total respondents. These areas are likely candidates for future growth in information security.

Security professionals who participated in the survey spanned a multitude of job functions and titles, ranging from Security Analyst to Chief Security Officer (CSO). Figure 1 shows that approximately 20% of all respondents were at the executive level (Chief Information Officer, Chief Information Security Officer, Chief Security Officer, Chief Risk Officer), Another 20% identified themselves as an IT director or manager, and the remainder identified themselves as a security practitioner, be it a 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 to security management to hiring staff. Individuals with sole responsibility for physical security were not included in this study.

[1] The forecast presented in this study represents Frost & Sullivan's best estimates and projections for 2007-2012 based on secondary Frost & Sullivan research from reported and observed trends and events in 2007. Predictions can be influenced by future segment-specific developments, including the unanticipated impacts of customer behavior, supplier actions, market competition, and relevant changes in the regulatory environment.

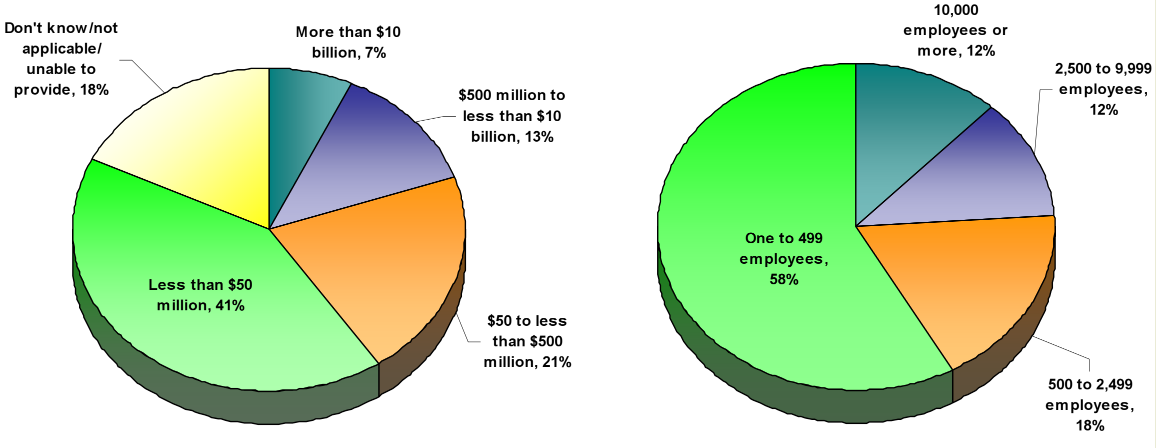
Figure 1 - Respondents by Job Title



Base: n=7,548 (ISC)² members and non-members

Information security professionals surveyed this year represent organizations of all sizes. Small organizations (one to 499 employees) accounted for more than half of the respondents (58%). Organizations with more than 500 but less than 10,000 employees employ approximately one-third of respondents, and companies with more than 10,000 employees (see Figure 2) employ just over 10%. Annual revenue was another criterion measured to gain a perspective on the types of organizations employing information security professionals. A total of four out of 10 organizations generate less than $50 million in revenue annually. Those organizations generating more than 10 billion in annual revenues employ 7% of respondents.

Figure 2 - Respondents by Company Size and Revenue

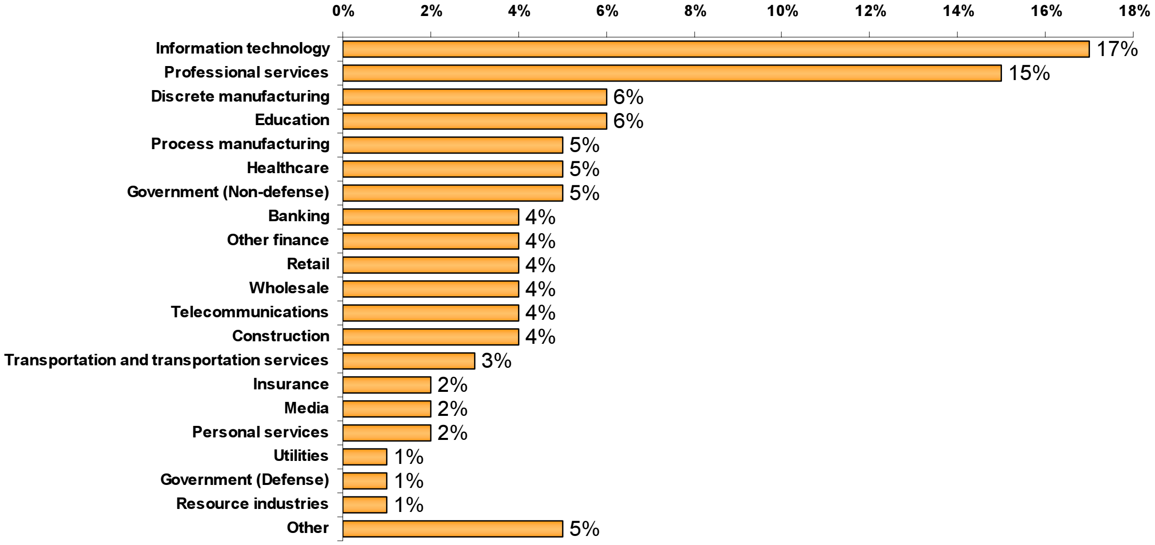


Base: n=7,548 (ISC)² members and non-members

Frost & Sullivan believes that the large number of professionals working for small organizations is reflective of several trends being observed throughout the industry. First, as all business continues to have an online component, organizations of all sizes are finding security to be a concern, whether they are protecting customer data or their own employees. Secondly, the last two years in particular have shown an increase in the number of regulatory compliance initiatives that affect organizations of all sizes. Directives such as PCI DSS are both global in scope and affect a wide range of organizations that are addressing security challenges for the first time.

From a vertical perspective, information technology and professional services are the top two industries employing information security professionals (see Figure 3). The continual addition of industry-specific regulatory mandates and varying access to resources such as capital and staff continue to force each industry and size of organization to address their information security needs with the right balance of risk versus cost. This balance is continually more challenging to maintain as the need for security permeates more aspects of the organization's operations.

Figure 3 - Respondents by Verticals

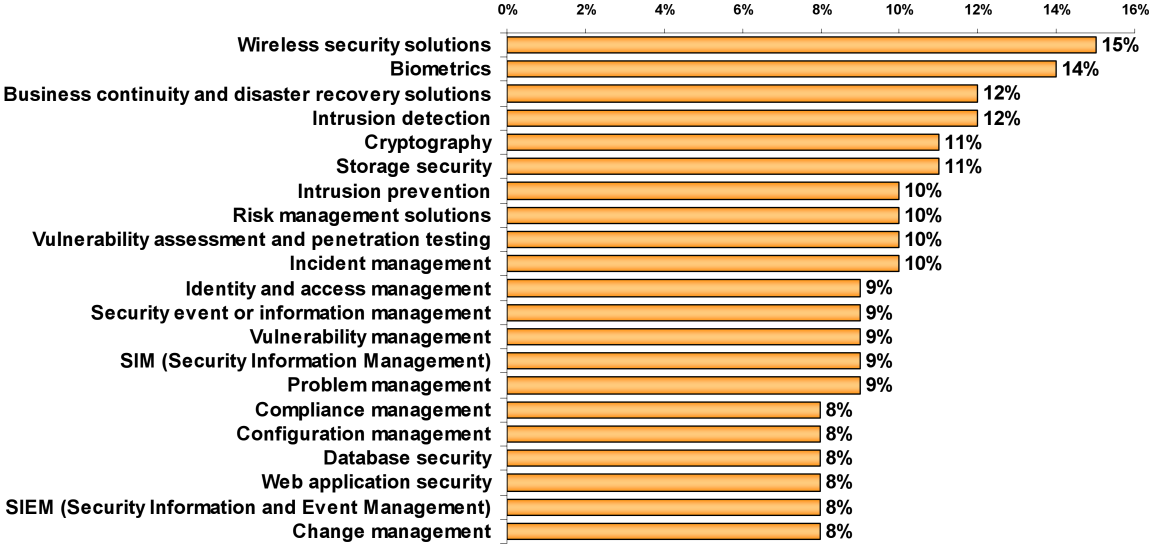


Base: n=7,548 (ISC)² members and non-members

ACCOMPLISHING SHORT-TERM GOALS

Information security professionals report that researching new technologies is where they spend the majority of their time. In many cases, this reflects that information security professionals are being tasked to secure the new technologies that organizations are planning to deploy. Figure 4 shows the top technologies that respondents reported their organization is planning to deploy within the next 12 months.

Figure 4 - Information Security Technologies - Planned for Deployment



Base: n=7,548 (ISC)² members and non-members

Some common security technologies being implemented across the regions are wireless security, biometrics, intrusion prevention, cryptography, and disaster recovery/business continuity. Frost & Sullivan believes that these focus areas (shown in Table 2) represent some of the greatest vulnerabilities in most organizations.

The reporting of the deployment of wireless security and biometric solutions is consistent with last year's findings. As the number of wireless access points and mobile devices continues to increase and incidents such as the TJX breach in the U.S. in particular illustrates, organizations have become increasingly concerned about wireless security solutions. The interest in biometrics shows the continued necessity for organizations to provide updated and improved access controls at appropriate levels to protect the organization's information assets and customer data protection. As privacy increasingly becomes required for regulatory compliance, the increased interest in biometrics comes as no surprise.

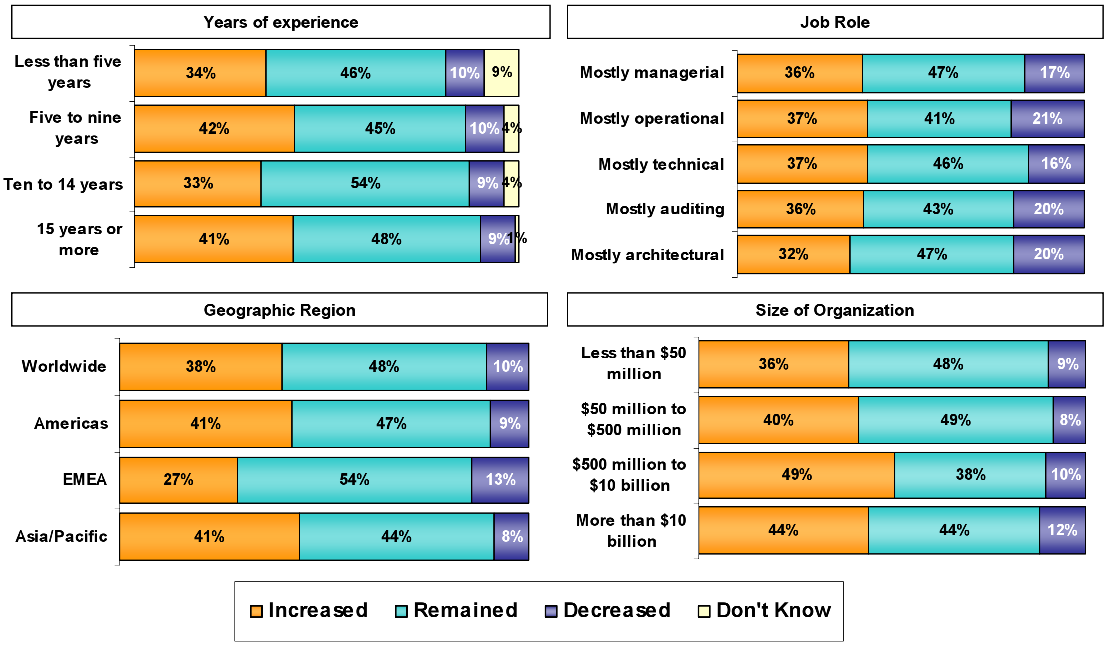
Table 2 - Top Five Security Technologies Being Deployed by Region

Rank	Americas	Asia-Pacific	EMEA
1	Biometrics	Wireless security solutions	Wireless security solutions
2	Wireless security solutions	Intrusion detection	Storage security
3	Business continuity and disaster recovery solutions	Business continuity and disaster recovery solutions	Biometrics
4	Intrusion detection	Biometrics	Risk management solutions
5	Cryptography	Cryptography	Business continuity and disaster recovery solutions

To effectively deploy solutions, organizations must continue to spend adequate dollars on personnel to meet organizational security goals. Respondents report information security spending on personnel has remained stable in the Americas and EMEA in 2007 compared to 2006. In contrast, Asia-Pacific respondents anticipate an increase in information security spending across the board. 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 by this figure.

Figure 5 highlights regional differences in funding security staffing requirements since 2006 based on years of experience, job role, geographic region and size of organization. Geographically, 31% of respondents in the Americas and Asia-Pacific reported that spending increased, while 27% of respondents in EMEA reported an increase. A large number of respondents in all three regions, indicated that training spending stayed the same since 2006 [nearly 50% in the Americas and Asia-Pacific and over 60% in EMEA]. Professionals with five to nine years of experience working for organizations with $500 million to $10 billion in revenues reported the largest increase in the amount of training they received in 2007.

Figure 5 - Changes in Information Security Training and Education (12-month Period)



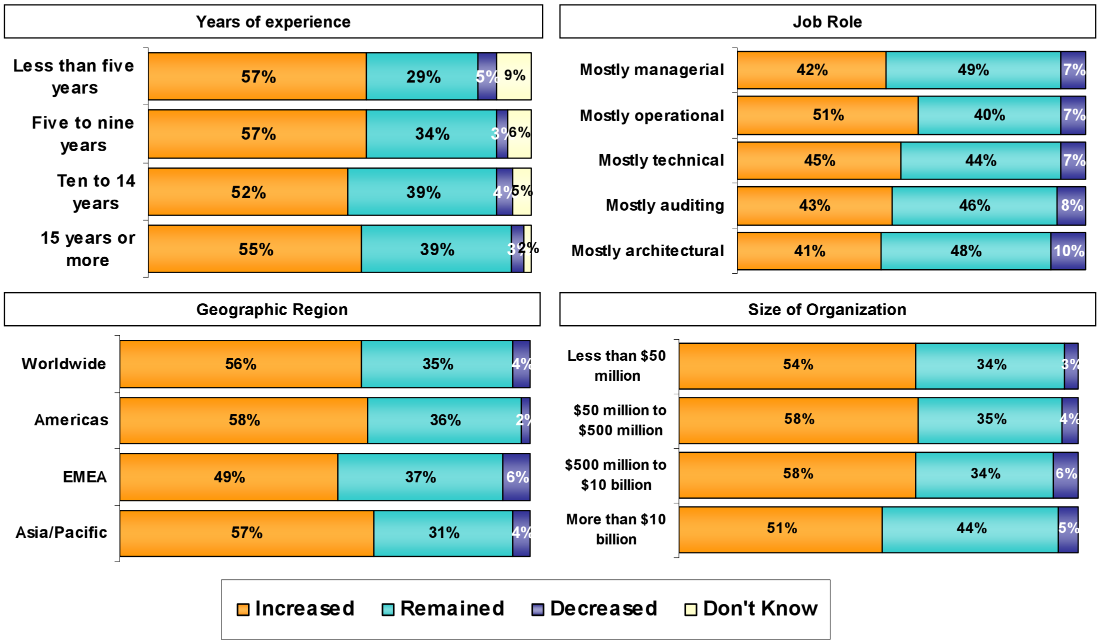
Base: n=7,548 (ISC)² members and non-members

Looking ahead, professionals were very optimistic that there would be increases in budget for training in 2008 (see Figure 6). Almost 60% of respondents with less than 10 years of experience reported an expected increase in training dollars. Additionally, more than 51%

of respondents in operational roles reported an expected increase in training budgets. Nearly 60% of respondents in the Americas and Asia-Pacific reported they expect training and education to increase in the next 12 months. Finally, respondents working for companies generating up to $10 billion in revenues reported an expected increase.

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

Figure 6 - Expected Change in Budget for IT Security Spending (12 months)



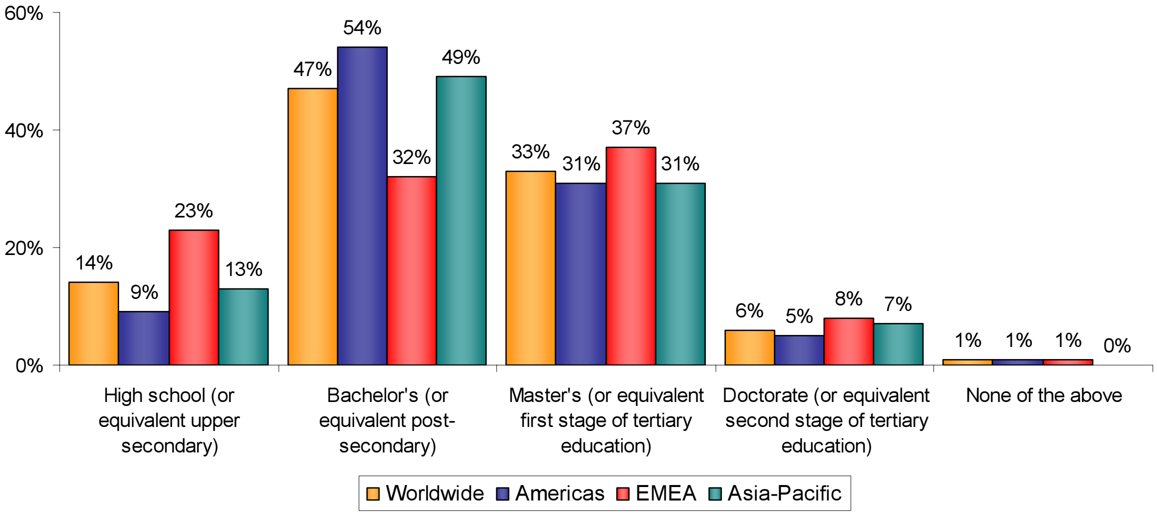
Base: n=7,548 (ISC)² members and non-members

PROFILE OF AN INFORMATION SECURITY PROFESSIONAL

From a professional development viewpoint, as in past years, respondents reported achieving a high level of education (see Figure 7). More individuals with at least a bachelor's degree or equivalent are employed in information security. Worldwide, 47% of information security professionals have a bachelor's degree or equivalent, with the Americas and Asia-Pacific having the highest number, at 54% and 49% respectively. However, EMEA reported both the highest number of professionals who hold master's and doctorate level degrees (37% and 8% respectively), with the Americas and Asia-Pacific tied at the master's degree level (31% each) and Asia-Pacific having slightly more professionals holding doctorate degrees than the Americas (7% compared to 5%).

Frost & Sullivan believes that the increasing education level of respondents points to the increasing maturity of the field. As universities develop specialized programs at the bachelor's, master's and even doctorate levels, information security practitioners are likely to feel increased pressure to pursue more and more specialized education. Hiring managers will have to balance the education gained from a formal classroom with experience gained from the field.

Figure 7 - Education Level by Region



Base: n=7,548 (ISC)² members and non-members

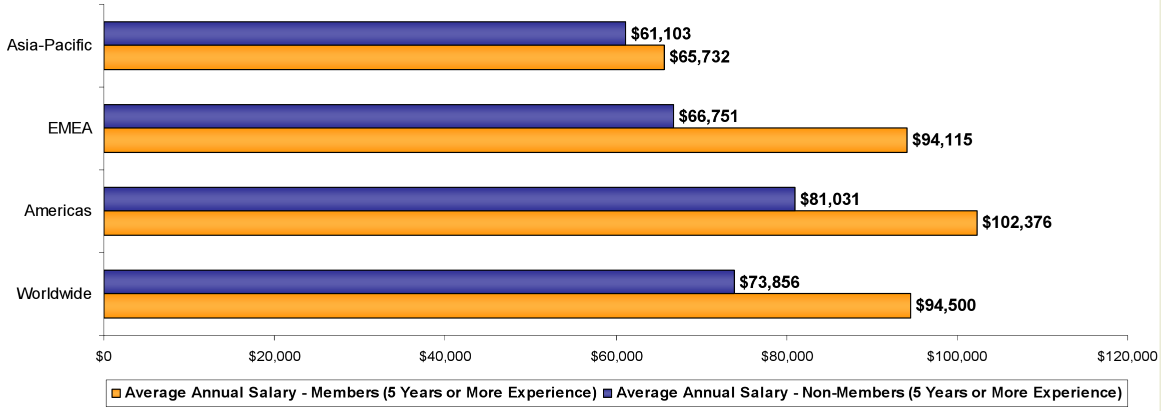
Years of professional experience proved to be another important candidate criterion for hiring managers and their organizations as a complement to or substitute for education. With a maturing workforce and new entrants fulfilling the staffing needs in organizations, some shifts have occurred across reported experience segments. In 2007, security professionals in the Americas averaged 9.5 years of experience, while security professionals in EMEA and Asia-Pacific averaged 8.3 years and 7.1 years, respectively. The Americas region hosts professionals with the most information security experience. The increasing numbers in these regions show that information security professionals are staying in their roles.

With more individuals achieving higher education levels and gaining valuable experience, information security salaries this year have shifted globally to reflect some of the regional dynamics taking place.

Frost & Sullivan also saw a significant difference in the salaries reported by (ISC)^2 members – information security professionals holding an SSCP®, CISSP®, or CAP® certification – compared to information security professionals that 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), there are significant differences in salaries across the regions.

This difference in salary ranged from 7% in Asia-Pacific to nearly 30% in EMEA. There are a number of factors that contribute to these differences, most notable of which is the number of experienced professionals in each region. Asia-Pacific has a relatively inexperienced workforce and few professionals are over the five- year mark.

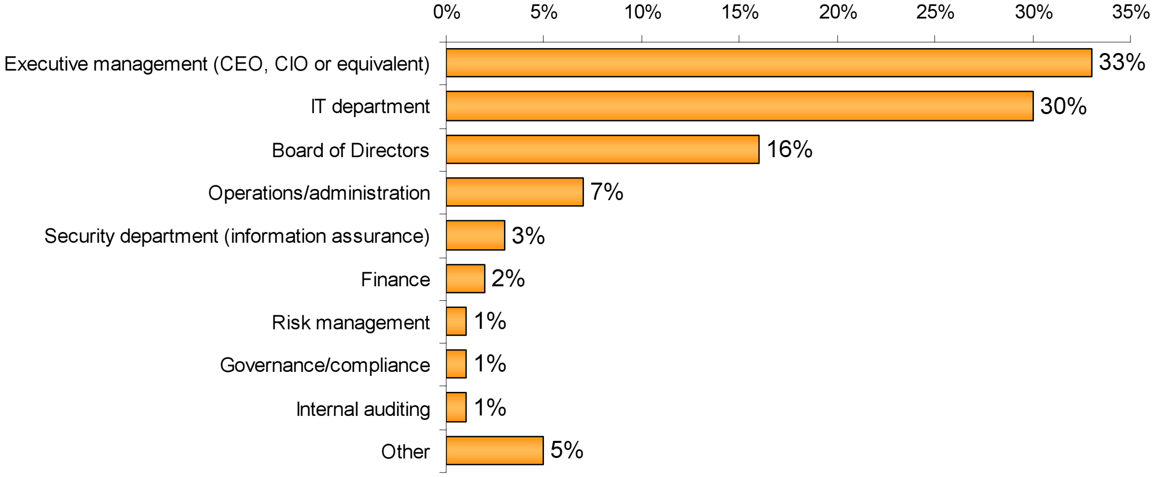
Figure 8 - (ISC)^2 Member versus Non-member Survey Comparison of Average Annual Salary by Region (5+ Years of Experience)



Base: n=7,548 (ISC)^2 members and non-members

Reporting lines for the majority of information security professionals worldwide have not changed dramatically over the course of the past 12 months (see Figure 9). Three out of every 10 still directly report into the IT department, which is slightly less than the 32% reported in 2004 and 2005. In 2007, however, the number of professionals reporting to executive management rose to 33%, showing the increasing visibility at the executive level. Other groups such as risk management, internal auditing, and governance/compliance have become more established in organizational hierarchies over the past two years given the escalating regulatory environment globally. Frost & Sullivan continues to see an increased number of regulations with a more global reach. Some of these include PCI, EU Directive 2002/58/EC, and ISO 27001/27002. These standards and other regional standards such as the India Technology Act and the Australian Privacy Act will force executive level support of information security initiatives as part of doing business globally.

Figure 9 - Functional Area Respondents Report To



Base: n=7,548 (ISC)^2 members and non-members

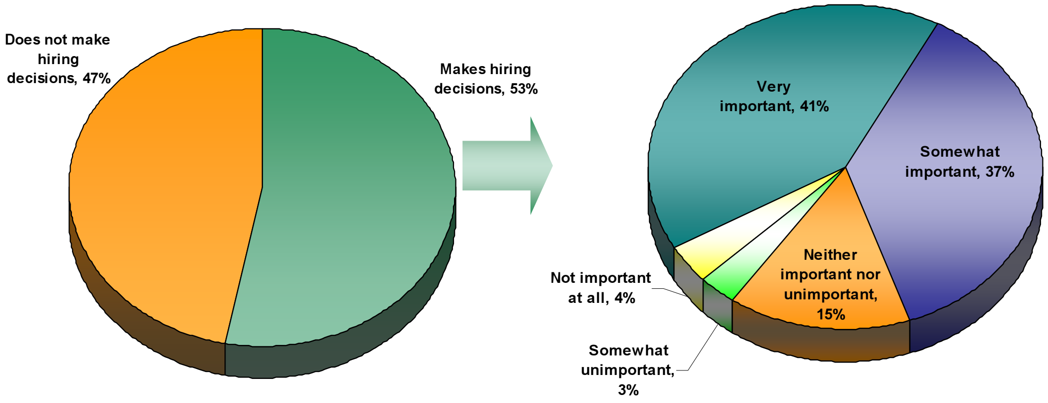
THE VALUE OF INFORMATION SECURITY CERTIFICATIONS

Twenty years ago, very few professionals had "practical" experience securing a network, as it was a new area of IT and not a well-understood discipline. Only the highest security networks were seen as even needing security; therefore, few professionals existed. Ten years ago, organizations and hiring mangers began to realize the importance of information security as a skill. There were, however, still a very limited number of experienced professionals. As a result, hiring managers began relying upon certifications as a criterion for hiring an employee in lieu of experience. Attaining a security certification made an important statement to potential employers that an individual had sought out the knowledge, skills, and abilities to defend an organization against possible breaches and build up defenses. This achievement placed candidates ahead of their peers, as additional metrics beyond certification were not available.

According to the 53% of survey respondents identified themselves as being involved in the hiring process for information security staff within their organizations, the importance of information security certifications as a hiring criterion remained high, with 78% of hiring managers citing certifications as either “Very Important” or “Somewhat Important” (see Figure 10).

Figure 10 - The Importance of Information Security Certifications When Hiring

Are you currently responsible for hiring your organization's staff that are dedicated to information security activities?
IF YES - When making hiring decisions for information security staff, how important is it for the candidate to have information security certifications?



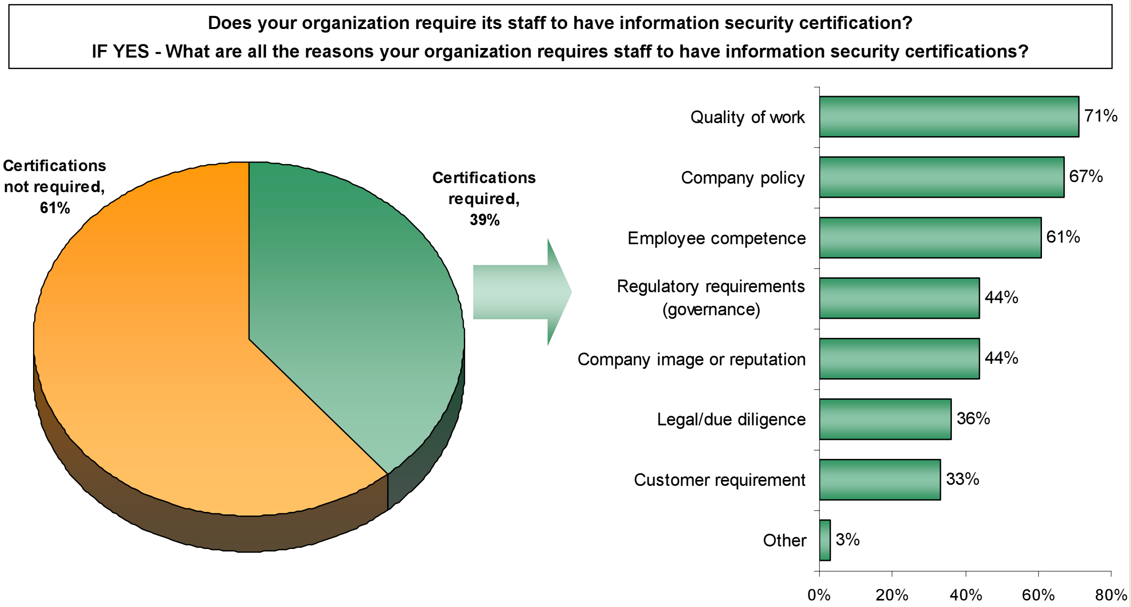
Base: n=7,548 (ISC)² members and non-members

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

There are certification programs that employ rigorous development standards and require a significant amount of education, experience and in-depth knowledge of information security. Certification providers will need to highlight the rigors, qualifications, years of experience, continuing education and other steps to attain and maintain their certifications. In the end, information security professionals will decide which certifications are of value to them.

As they pertain to the candidate selection criteria of the organization, top reasons managers prefer to hire information security professionals with information security certifications are illustrated in Figure 11. Quality of work, company policy, and employee competence remain the major reasons; however, others are surfacing. As this year's study showed, more organizations are requiring their information security staff to hold certifications because of company policy and regulatory compliance. In the Americas, hiring managers are feeling the pressures of regulatory compliance and want to ensure their information security staffs are knowledgeable and skilled and carry the credentials to get them to compliance. One example in the U.S. is the Department of Defense (DoD) Directive 8570.1, which requires all DoD information assurance technicians, managers and contractors to be trained and certified to a DoD baseline requirement. Thirteen certifications have been identified and mandated by the Directive's enterprise-wide certification program, including (ISC)^2 certifications.

Figure 11 - Main Reasons for Staff to Have Information Security Certifications



Base: n=7,548 (ISC)^2 members and non-members

Even though having a certification should not be the single qualification for an information security professional, the increasing number of companies with stated policies regarding the hiring of certified professionals and the increasing number of compliance directives that specify the need for a certification (such as the DoD Directive 8570.1 in the U.S. federal government) increase the importance that will be placed on information security certifications in the future.

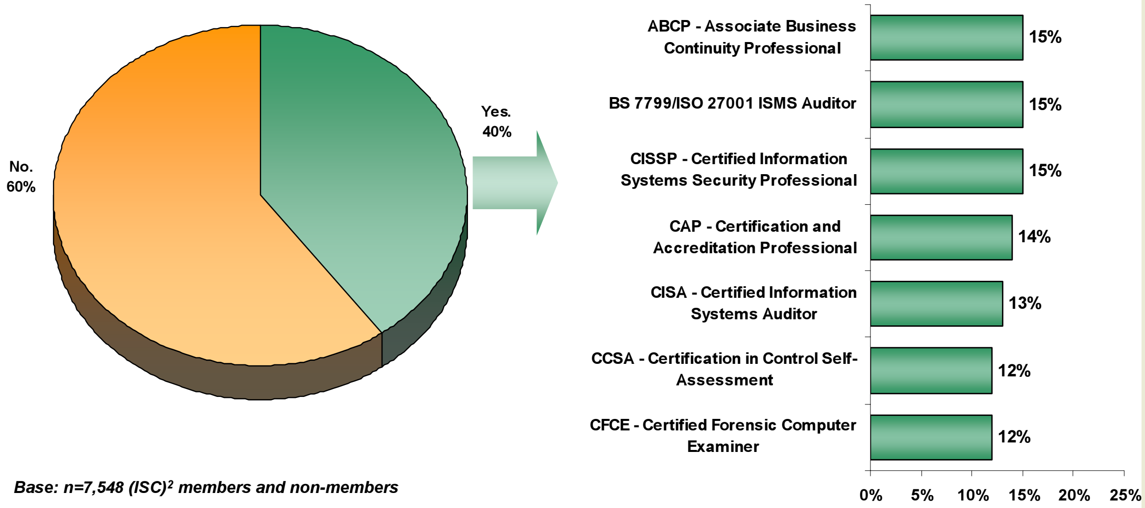
CONTINUING EDUCATION EXPECTED FOR INFORMATION SECURITY PROFESSIONALS

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

Differentiation from other candidates and potential salary benefits have been other reasons individuals interested in information security obtain certifications. These additional benefits continue to be enjoyed by information security professionals, as demonstrated in the results throughout this study. In an effort to guarantee that they remain relevant, 40% of respondents said they would look for at least one more new certification to add to their toolkits in the 2007-2008 period (see Figure 12).

Figure 12 - Plans to Acquire Additional Certifications

Are you planning to acquire additional security certifications in the next 12 months?
IF YES - Which additional vendor neutral security certifications are you planning to acquire or renew in the next 12 months?



Base: n=7,548 (ISC)^2 members and non-members

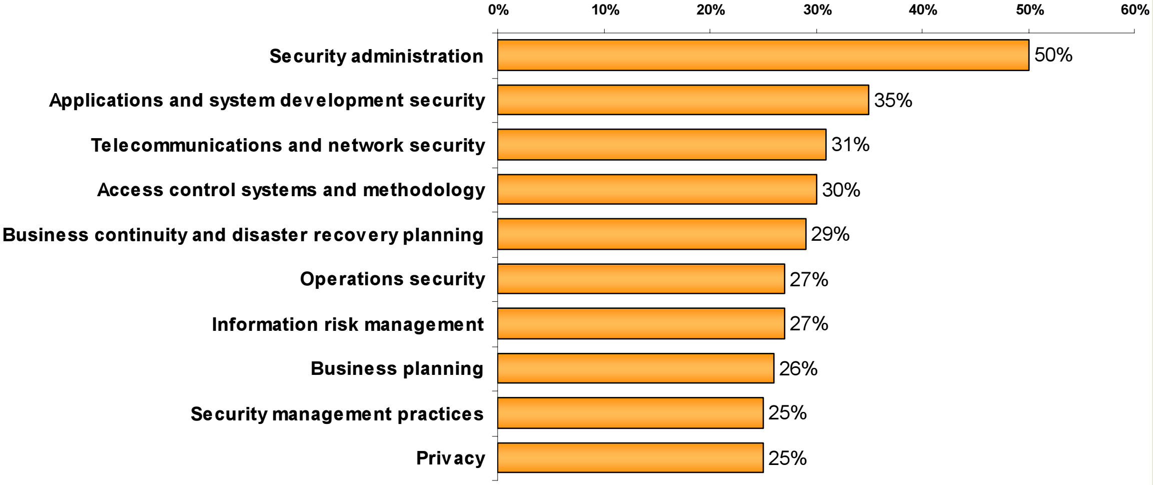
In the future, security professionals must stay on top of the latest technologies and best practices through continuing education and practical experience to deal with the evolving computing environment (e.g., virtualization and service-oriented architecture) and the changing nature of information security. Organizations are moving toward a converged security environment in which physical and logical security operate over a single network. Technical knowledge will be important; however, knowing the business and utilizing business skills, such as communication, negotiation, and managing up and down, will become even more critical to an individual's career advancement and survival.

LOOKING AHEAD

Future Education 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 security administration (see Figure 13). As organizations implement new technology solutions, the need for increased training and education as how to securely administer those systems is very important.

Figure 13 - Growing Need for Training



Base: n=7,548 (ISC)² members and non-members

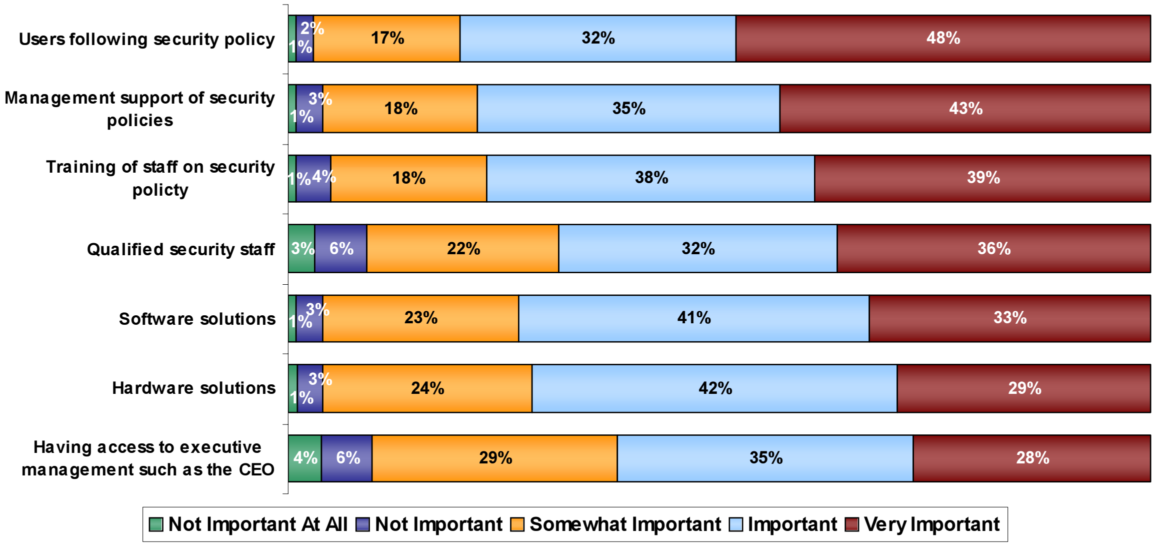
Frost & Sullivan believes that application and system development and security will continue to be a critical area of investment for organizations in the future. Many organizations are coming to the realization that their own internal systems suffer from the same security risks as those coming from a vendor.

Technology Alone Will Not Fix the User Problem

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

More and more, executive management is starting to buy into and own information security for their organizations. Information security professionals have remained positive about their ability to influence and have been instrumental in changing the mindset of executives and gaining their buy-in that security is an enterprise-wide problem, not just an IT issue (see Figure 14).

Figure 14 - Relative Importance to Secure the Organization



Base: n=7,548 (ISC)^2 members and non-members

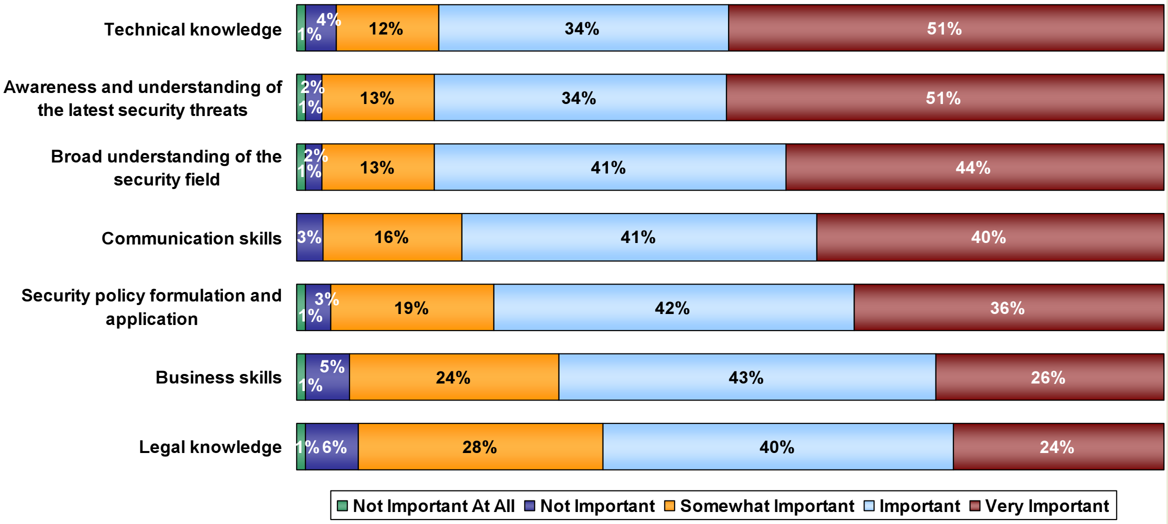
Much of information security professionals' time will be spent meeting with executives and management to discuss the significance of corporate security policies and why they should be implemented and, more importantly, enforced. According to the 2008 study, this is security professionals' primary concern for effectively securing their organizations' infrastructures. The following list shows the factors (from most important to least important) affecting information security professionals' ability to properly protect and secure the computing infrastructure and its resources from breaches, misuse, and abuse:

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

This list is unchanged from the 2006 survey and shows the continued emphasis on the people aspect of security, one of the primary areas that has often been overlooked in the past in favor of deploying more technology to solve security problems. Information security professionals in each region unanimously acknowledged that technology is only an enabler, not the solution, to executing a sound security strategy and supporting a welldefined and well-articulated risk management program where all stakeholders share responsibility.

Respondents also cited communication skills as one of the top five skills needed to be a successful information security professional (see Figure 15). Frost & Sullivan believes this reflects the realization by executives that technology solutions are not enough to solve an organization's security problems. Information security professionals are tasked to perform more education and training functions within organizations. This requires a versatile workforce with both technically diverse skills and the ability to convey security basics to a non-technical audience.

Figure 15 - Importance of Information Security Skills



Base: n=7,548 (ISC)^2 members and non-members

CONCLUSION

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

Frost & Sullivan believes that the 7,548 information security professionals who shared their views and opinions in this study are the security evangelists within their organizations. These respondents fully understand that security is now a critical component in the operation of the modern organization. It is the duty of information security professionals to ensure information security is recognized for its positive contributions to the business, as opposed to the sunk cost it has been perceived to be in past years. The message of people and processes being absolutely crucial to effective information security is finally starting to resonate with business leaders. As a result of the 2008 GISWS, Frost & Sullivan advises information security professionals to consider the following conclusions:

- Emerging markets (Latin America, Africa, and Oceania) offer attractive employment opportunities for information security professionals over the next five years.

- Compliance is driving organizational behavior from changes in spending levels to shifts in accountability to requirements in new skill sets.

- Security domains such as security administration, business continuity, and secure application development are topics where professionals are looking to increase their knowledge and sharpen their skills.

- Senior executives remain ultimately accountable for security and risk management; however, others, such as the CRO and CISO are shouldering the burden of accountability, along with the CIO, CEO, and board of directors.

- Customer and public confidence will drive security up the priority list, based on the increasing impact that evolving threats have on the reputation and issues relating to privacy violations.

- People and processes finally become recognized as the greater focal point for risk management efforts as technology is acknowledged to be an enabler for achieving organizational objectives, not the solution.

- Certifications with rigorous education and work experience requirements will continue to be an important differentiator as the number of professionals necessary to effectively secure organizations continues to increase.

CONTACT US

Palo Alto

New York

San Antonio

Toronto

Buenos Aires

Sao Paulo

London

Oxford

Frankfurt

Paris

Israel

Beijing

Chennai

Kuala Lumpur

Mumbai

Shanghai

Singapore

Sydney

Tokyo

Silicon Valley
2400 Geng Road, Suite 201
Palo Alto, CA 94303
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

ABOUT FROST & SULLIVAN

Frost & Sullivan, the Growth Consulting Company, partners with clients to accelerate their growth. The company's Growth Partnership Services, Growth Consulting and Career Best Practices empower clients to create a growth focused culture that generates, evaluates and implements effective growth strategies. Frost & Sullivan employs over 45 years of experience in partnering with Global 1000 companies, emerging businesses and the investment community from more than 30 offices on six continents. For more information about Frost & Sullivan's Growth Partnerships, visit http://www.frost.com.