



## NEWS

### FOR IMMEDIATE RELEASE

**Note to Editors:**

To request a copy of this study or individual country data cut, please contact:

Kitty Chung  
(ISC)<sup>2</sup> Asia-Pacific  
(852) 3520-4001  
kchung@isc2.org

## PEOPLE AND PROCESSES MORE IMPORTANT THAN TECHNOLOGY IN SECURING THE ENTERPRISE, ACCORDING TO GLOBAL SURVEY OF 4,000 INFORMATION SECURITY PROFESSIONALS

*3<sup>rd</sup> Annual (ISC)<sup>2</sup>-Sponsored Global Information Security Workforce Study says Asia-Pacific offers attractive employment incentives and opportunities for information security professionals*

**Hong Kong, Oct. 26, 2006** – The International Information Systems Security Certification Consortium [(ISC)<sup>2</sup>®], the non-profit global leader in educating and certifying information security professionals throughout their careers, today announced the results of the third annual Global Information Security Workforce Study, conducted by global analyst firm IDC and sponsored by (ISC)<sup>2</sup>.

According to more than 4,000 information security professionals in more than 100 countries in the largest study of its kind, the most important elements in effectively securing their organization's infrastructure are (in order of importance):

- Management support of security policies
- Users following security policy
- Qualified security staff
- Software solutions
- Hardware solutions

According to the study, the top three success factors highlight the need for public and private entities to focus more time and attention on policies, processes and people, all areas which have been traditionally overlooked in favor of trusting hardware and software to solve security problems. Survey respondents say organizations are now beginning to recognize that technology is an enabler, not the solution, for implementing and executing a sound security strategy.



The study also found that responsibility for executing a sound security strategy is being increasingly shared across the organization, making C-level officers accountable as part of a well-defined and articulated risk management program. Continuing a trend identified in last year's study, responsibility for securing information assets is shifting from the Chief Information Officer (CIO) into other areas of senior management and business, including chief executive officer, chief financial officer, chief risk officer and chief information security officer, as well as legal and compliance departments.

“For organizations to proactively secure and protect their infrastructure, information, financial and physical assets requires the unconditional commitment to security at the financial, management and operational levels,” said Allan Carey, program manager at IDC who led the study. “Security management will always require the proper balance between people, policies, processes and technology to effectively mitigate the risks associated with today's digitally connected business environment.”

IDC analyzed responses from 4,016 full-time information security professionals in more than 100 countries, with nearly 40 percent employed by organizations with US\$1 billion or more in annual revenue. Respondents came from three major regions of the world: North, Central and South America (57.3%), EMEA (Europe, Middle East, Africa) (22.8%) and A-P (Asia-Pacific, including Japan) (19.5%), and represent organizations of various sizes from both the public and private sectors, different vertical industries, and varying core competencies and skill sets from organizations. Respondents typically had purchasing, hiring and/or management responsibilities. Other highlights from the 2006 study include:

- IDC estimates the number of information security professionals worldwide in 2006 to be 1.5 million, an 8.1 percent increase over 2005. This figure is expected to increase to slightly more than 2 million by 2010, displaying a compound annual growth rate (CAGR) of 7.8 percent from 2005 to 2010. As a comparison, the projected growth in the number of IT employees globally in the same timeframe is 4.6 percent.
- A-P presents the highest growth opportunities for information security professionals over other regions. IDC estimates the number of information security professionals in A-P to grow from 458,844 to 733,943, representing CAGR of 9.8 percent from 2005 to 2010. The growth for 2005-2006 has been 10.6 percent.
- A-P salaries have progressed and are starting to come inline with other regions of the world. For individuals earning between US\$70,000 and \$125,000, there was a 6.2 percent positive difference between 2005 and this year. On the lower end of the spectrum, security professionals in A-P earning less than US\$40,000 still consist of more than 39 percent of all respondents in the region; however, this is seven percent fewer than last year, which was on par with 2004.
- A-P tends to lag the US by approximately 18 months when it comes to information security market maturity, therefore, A-P is now experiencing above average growth that occurred in the US four to five years ago.



- Common security technologies being implemented by organizations across all regions are biometrics, wireless security, intrusion prevention and forensics tools. Biometrics ranked either No. 1 or 2 across all regions.
- The area of information security risk management has risen to the top as a training priority in both the Americas and EMEA and is No. 2 in A-P. This will continue for the foreseeable future as organizations struggle to gain control over their risk posture, develop a flexible framework to quickly adapt to new environmental factors, and provide visibility into their greatest risks. Business continuity and forensics are also topics where professionals are looking to increase their knowledge base and sharpen their skills.
- During the past 12 months, 67 percent of security practitioners believe their efforts were effective in influencing management and the business stakeholders to drive security awareness and responsibility to their organizations. Looking forward to 2007, 73 percent believe that they will be able to drive change in their organizations.
- Overall, organizations are spending a greater percentage of their information security budgets on personnel and training in 2006 than in 2005. Organizations are spending more than 41 percent of their security budgets, on average, on personnel and training to staff projects and support post-deployment management.
- The importance of information security certifications as a hiring criterion remained high with 85 percent of hiring managers but was down from a peak of 92 percent in 2004.

“IDC believes that the security professionals who participated in this study are taking their message to the masses and acting as ‘change agents’ within their organizations to ensure information security is recognized for its positive contributions to the business, as opposed to the sunk cost it has been perceived to be in past years,” Carey said. “The message of people and processes being absolutely crucial to effective information security is finally starting to resonate with business leaders.”

“Security breaches that have made headlines during the past year have been a result of human error, and this year’s Global Information Security Workforce Study further validates the conventional wisdom long-held by information security professionals that people are the critical component of an effective information security program,” said Ed Zeitler, CISSP, executive director, (ISC)<sup>2</sup>. “The fact that professionals are being heard by the C-suite and security responsibility is being shared across the organization demonstrates that the information security profession has arrived and is being valued as an indispensable business component.”

“In regard to certification, this survey did not differentiate between certifications that rely on a test solely and those that require validated work experience, continuing education, peer sponsorship and other requirements generally associated with professional certifications in other more established fields,” added Zeitler. “We believe accredited certifications that support management’s need for professionals with real-world experience and ongoing education are viewed more favorably than certifications earned for passing a test alone.”



The 2006 Global Information Security Workforce Study (IDC Doc # 203970, October 2006) was conducted by IDC on behalf of (ISC)² to provide detailed insight into important trends and opportunities within the information security profession. The study aims to provide a clearer understanding of how professionals are compensated, how their organizations view security, and next steps required to advance information security careers and the profession. To download a copy of the study, please visit [www.isc2.org/workforcestudy](http://www.isc2.org/workforcestudy).

#### **About (ISC)²**

The International Information Systems Security Certification Consortium [(ISC)²] is the premier non-profit organization dedicated to certifying information security professionals around the world. Founded in 1989, (ISC)² has certified over 45,000 information security professionals in more than 120 countries. Based in Palm Harbor, Florida, USA, with offices in Vienna, Virginia, USA, London, Hong Kong and Tokyo, (ISC)² issues the Certified Information Systems Security Professional (CISSP®) and related concentrations, Certification and Accreditation Professional (CAP<sup>CM</sup>) and Systems Security Certified Practitioner (SSCP®) credentials and related concentrations to those meeting necessary competency requirements. The CISSP, the CISSP-ISSEP® and SSCP® are among the first information technology credentials to meet the stringent requirements of ANSI/ISO/IEC Standard 17024, a global benchmark for assessing and certifying personnel. (ISC)² also offers a portfolio of educational related products and services based upon (ISC)²'s CBK®, a taxonomy of information security topics, and is responsible for the (ISC)² Global Information Security Workforce Study. More information about (ISC)² is available at [www.isc2.org](http://www.isc2.org).

###

© 2006, (ISC)² Inc. (ISC)², CISSP, ISSEP, SSCP and CBK are registered certification marks and CAP is a service mark of (ISC)² Inc.