FROST & SULLIVAN

Critical Times Demand Critical Skills

An analysis of the skills gap in information security

A whitepaper derived from the (ISC)² Global Information Security Workforce Study, a Frost & Sullivan market study in partnership with:

(ISC)²®

Booz | Allen | Hamilton

strategy and technology consultants

Background

The 2013 (ISC)²® Global Information Workforce Study found an ever widening gap between the supply of qualified information security professionals and the demand for skilled workers to secure critical information and the cyber world. The study shows that the workforce will grow at a compound annual growth rate of 11.3% globally between now and 2017, calling for an additional 2.0 million new workers.

2013 (ISC)² Global Information Workforce Study, conducted in partnership with Booz Allen Hamilton, with the assistance of Frost & Sullivan, is the sixth bi-annual (ISC)² worldwide survey of information security professionals. This Web-based survey, conducted in the fourth quarter of 2012, was both broad in scope (more than 12,000 respondents, a 19 percent increase over the 2011 survey) and deep in its queries.

Concerns about the gap in the workforce are not new; however, the issue is now acute. The 2013 study also shows an increase in threats driven by the rapid introduction of new technologies that don't have security "baked in" the product development process. In addition, the number of organized attacks is increasing as hackers move from individuals flexing their own skills to interconnected groups of criminals who share information and conduct coordinated attacks.

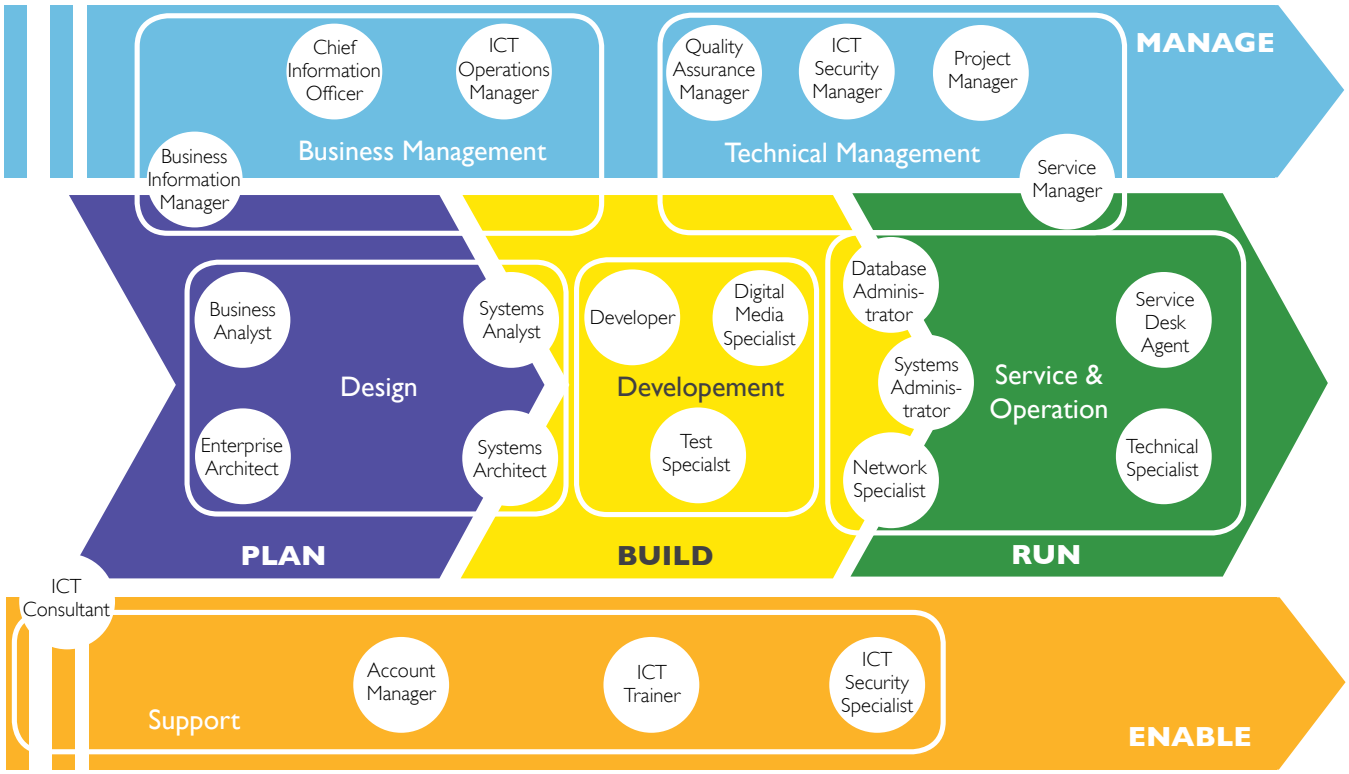
Yet, open information security positions are going unfilled; 56% of those responding to the survey feel their organizations currently have too few information security workers to manage threats now, let alone in the future. Just over 35% of survey respondents say they would hire additional workers, but find it difficult to find qualified personnel. A report from Burning Glass Technologies, an IT-driven recruiting firm, shows that demand for information security workers grew 3.5 times after than demand in other IT specialties over the last five years. Job postings in information security grew 73% between 2007 and 2012 (versus an average for all jobs of 6%) to a total of 67,400 in the US alone.

It's one thing to know there's a gap between the need for information security professionals and the supply of new, skilled workers. It's another thing to know the exact skill sets in highest demand. The field of information security is not monolithic; it's made up of a variety of skill sets involving a combination of technical, planning, and managerial skills. In this 6th edition of the (ISC)² Global Information Workforce Study, respondents were asked to be specific about the skill sets most needed to round out their information security teams. This report focuses on those skills sets most in demand overall as well as within specific industries, different sized companies, and various global regions.

Frameworks

A list of 39 job categories was used in the survey questionnaire to bring specificity to the gap in the workforce. The options given were reflective of a group of industry frameworks developed throughout the world with a focus on frameworks from the European Union and the USA's National Initiative for Cybersecurity Education (NICE), as well as constructs in use in the United Kingdom and Japan. The hope is that a more specific description of the most sought-after skills will lead to customized programs that can be used to develop workers with the exact skill sets needed, including university curricula, and government, industry association and private sector continuing education initiatives.

The **EU system** was developed by the European Committee for Standardization with input from governments, organizations, and professionals across the EU and includes 23 job profiles in six areas of IT security: business management, technical management, design, development, service and operations, and support. These jobs also cluster into five segments, each driven by an action verb: manage, plan, build, run, and enable.



The **NICE Cybersecurity Workforce Framework** outlines seven broad areas of practice within information assurance:

1. Securely provision
2. Operate and maintain
3. Protect and defend
4. Investigate
5. Operate and collect
6. Analyze
7. Oversight and development

Within each of these areas, specific job functions are described along with sample job titles, for a total of 31 different areas of practice.

Success Attributes

The 2013 $(ISC)^2$ Global Information Security Workforce Study uncovered that a diverse set of skills beyond technical skills in information security are needed to be successful. Across the entire survey, a broad understanding of the security field topped the list in terms of importance, and technical knowledge, awareness and understanding of the latest security threats are included in the top four skills necessary to excel in the field.

Higher order management skills are also needed, however. Communication skills (#1), policy formulation and application (#5), leadership, business management, and project management skills (#6-8), and legal knowledge (#9) are paramount for a successful career in information security.

"Most organizations operate symmetrically, but as infosec professionals, we work in an asymmetrical industry," said Sarah Bynum CISSP, CPP, Director of Security, Siemens Energy, Inc. "Threats can come from anywhere, enter our systems anyplace, and we need to develop people with skills sets that can handle an asymmetrical threat environment."

Factors Contributing to Success (Very Important and Important)

Respondents in the banking, finance, and insurance verticals place a higher emphasis on the importance of a broad understanding of security than other verticals. Information technology and government/defense place higher importance on technical knowledge. Healthcare respondents rate communication skills higher in importance.

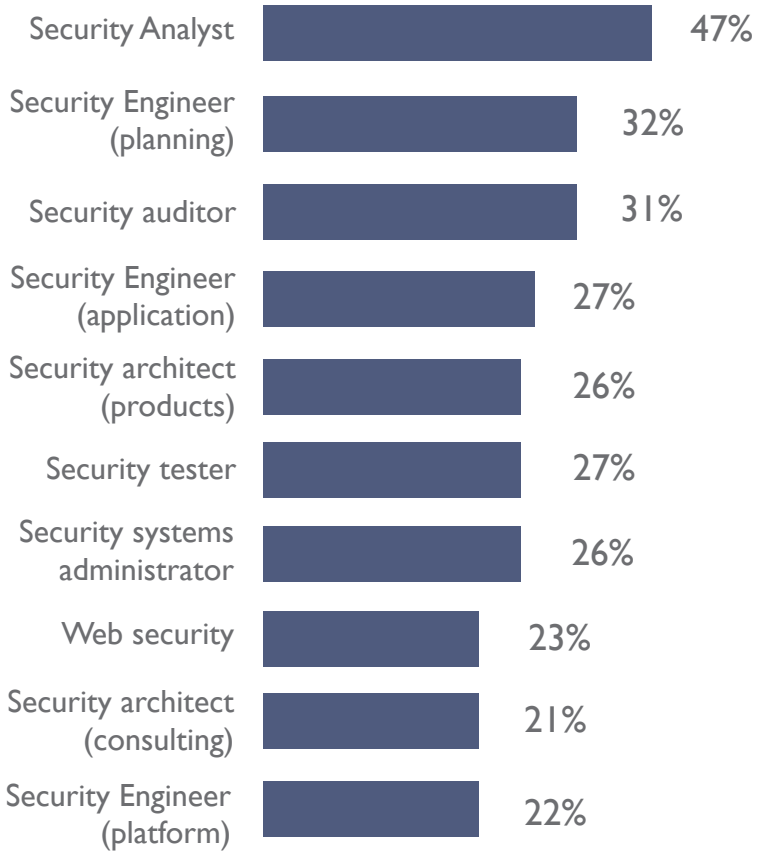
The Gap

Overall, the skill set most in demand is **Security Analyst** who conducts the integration and testing, operation, and maintenance of systems security, with 47% of respondents naming this position as their top need. In addition, a security analyst possesses significant higher order skills and has a deep understanding of all business systems, knowing what information an organization cannot afford to lose. They are proficient in cyber threat analysis and in identifying and assessing the capabilities and activities of cyber criminals or foreign intelligence entities. They may also analyze threat information from multiple sources and disciplines, synthesizing it and placing it into context while drawing insights about the possible implications, according to the NICE Cybersecurity Workforce Framework.

Three of the top ten job titles in demand are in Security Engineering (planning/design, applications, platform), indicating a growing understanding of the need to include security in the planning, design, and development of information security systems and processes, and in the development of new applications.

"The shortfall of staff with intelligence capabilities is a key finding of the study," said Bill Stewart, Senior Vice President, Booz Allen Hamilton. "This requires skills that bridge across a variety of areas of expertise to understand what the adversary is doing inside your network. More and more, the industry is moving toward creating intelligence and "hunt" capabilities to find sophisticated adversaries within networks, pointing to a significant demand for staff with the security analyst skill set."

Shortages by Job Titles (Top 10)



These findings are further supported by results of a focus group conducted by the University of Phoenix in conjunction with (ISC)[2], entitled "Competencies and Certifications for Information Security Careers: Highlights from an Industry Focus Group Discussion".

"Participants shared that individuals must have business analysis and acumen skills (the ability identify business needs, determine solutions to business problems, and make profitable business decisions)," states the report. "Diplomacy and negotiation skills (being able to deal with sensitive matters and find mutually-agreeable solutions to a common problem) were also reported as critical, as was the ability to conduct a risk assessment."

"Also shared as important to success were customer service skills, sales skills, and marketing skills, it continues. The ability to be assertive and forthright was also a reported necessary skill. Further, participants indicated that individuals must be able to prioritize, work in teams, and demonstrate confidence they can do something well or succeed."

"Several participants indicated that demonstrating cultural awareness (ability to pay attention to and adapt behavior to demonstrate culturally-appropriate behavior) was also an important skill."

When looking at the (ISC)[2] Workforce Study, responses from information security professionals working in governments around the world (military and nonmilitary positions), the rankings are nearly identical to those of the total sample, except for the need for Forensic Analysts. While the same number of total survey respondents and government respondents (20%) require the services of a **Forensic Analyst**, this position ranks within the **top ten** desired skills sets in government while ranking 13th within private industry. Forensic Analysts collect, process, preserve, analyze, and present evidence to support network vulnerability mitigation and/or breach investigations, according to the NICE Framework.

Specific Need of Industry Verticals

The greater priority for finding Forensic Analysts on the part of government has already been noted. Compared with other industries, they also have greater need for Security Engineers (planning and design, and requirements), Security Systems Administrators, Security Testers, and Incident Handlers. To some degree, this difference can be explained by the nature of the adversary. In organizations like governments where an attacker aims to gain a foothold in the network then remain there, undetected, for a long period of time for espionage activities, the need for forensics work is more significant.

Banking/insurance/finance, healthcare, and manufacturing are in significantly greater need of Security Analysts, but beyond that, their needs diverge: Healthcare companies also show a greater need for Incident Handlers and Web Security specialists.

Information technology companies find higher-than-average demand for Security Engineers with application experience and management consultants in security, while telecom and media companies have greater need for Security Engineers in both planning and design, and platform development, as well as Security Architects with products/solution experience.

Need by Company Size

Differences by company size can be explained in part by the need, in general, for smaller organizations to require their information security personnel to have more well-rounded skill sets, while larger organizations require personnel that are highly skilled within more narrowly defined areas of practice. For instance, companies employing between 500 and 2,499 people are most in need of security leadership, with 18% of them reporting the need for a CSO/CISO/CAIO (compared with 13% of the total sample). The smallest employers (those with fewer than 500 employees) are least likely to need a Security Analyst (37% compared with 47% of the general sample); they are more likely to need a Network Administrator (16% versus 12% of the total sample) or a Software Developer (8% versus 6% for larger companies). They are also more likely to need outside help from consultants than companies with 500-9,999 employees including Security Consultants (17% versus 13%), Technical Consultants (8% versus 4%), and Sales Consultants (5% versus 2%).

The largest companies, those with over 10,000 employees, are more likely to need engineering and architecture help in a variety of areas including applications (31% versus 27% of the total sample), requirements (20% versus 17%), product architecture (32% versus 26%) and consulting services in architecture (26% versus 21%). In addition, large companies are more likely than their smaller compatriots to need a Security Strategist (24%).

Differences by Respondent Title

When examining the need for additional information security personnel by the job title of the respondent, not surprisingly, C-Levels/Officers think they need more C-Level help; Auditors think they need more Auditors and Security Testers; and Architects, Strategists, and Strategic Advisors, yes, think they need more Architects, Strategists, and Strategic Advisors. The additional personnel needs expressed by those with management titles, while not dominating the sample size, fell in line with the needs of the overall sample.

Regional Differences

Several regional differences emerged in the data as well. In some instances, it means a more focused need on the global top ten positions, but in many cases, the need for staff diverges from the global average. Note that the survey was available in a variety of languages, thus a misinterpretation of the job titles due to language barriers is unlikely.

Americas

Findings in the Americas generally follow the pattern of the global results with a few notable exceptions. Software Developers, Architects, and QA Engineers are in high demand in **Mexico**, and the need for Forensic Analysts is more than double that of the global sample (44%). This may be due to Mexico's data protection law driving increased security in the software infrastructure in order to achieve compliance.

Also notable is **Brazil's** need for leadership in information security in the form of Security Management Consultants and CSO/CISO/CAIOs, potentially driven by Brazil's exploding economy. **Canadian** respondents indicate a need for Security Analysts that's nearly a third higher than the global sample, potentially driven by the trend toward CISOs taking on a larger risk management function and thus needing skilled professionals with broad experience in security analytics.

Europe, Middle East and Africa

Respondents in France and the **Middle East** indicate a greater than average need for additional security leadership in the form of CSO/CISO/CAIO and Deputies. Respondents in the **Middle East** also indicate a desire for additional staff in Security Auditing, Security Testing, Forensic Analysts, and Incident Handling. **German** information security professionals feel a greater than average need for staff with skills as Security Architects with specialties in products and solutions as well as consulting. They also need Security Advisors. This may be driven in part by the shift across EMEA from reactive to proactive security management as companies appreciate the value of building systems with security in mind, perhaps prompting the need for the kinds of skills possessed by Analysts and Advisors.

The greatest divergence from the global and regional sample came from respondents in South Africa. While five of their top ten needs align with global information security hiring needs, there's also a desire to add staff with skills as Security Testers, Security Architects with consulting experience, Security Advisors, and Web Security.

Asia-Pacific

Information security professionals in **Australia** identified a significantly greater than average need for Security Architects with a skill set in products/solutions and consulting. No other APAC nation showed this preference. **Chinese** respondents to the survey said they were most in need of Security Auditors, CSO/CISO/CAIO, and Security Engineers with a focus on database development and management.

Indian respondents also show a high demand for Security Auditors, but also need more workers with special skills as Security Strategists. Respondents from **Singapore** also show higher than average demand for Security Strategists.

Respondents in **Japan** and **South Korea** diverged the furthest from the global average responses when asked which skill sets they desired the most when adding staff to their teams. In **Japan**, Security Strategists were most in demand, followed by Security Systems Administrator, Security Management Consultant, Security Engineer with a specialty in requirement definition, and Incident Handler, perhaps driven by the number of recent incidents in Japan. This has also driven a shift toward a proactive, enterprise risk perspective from a reactive stance.

South Korean information security professionals with hiring responsibilities are focusing their hiring efforts on professionals with skills as Privacy Specialists and Privacy Officers, which is the first country where we've seen a need for professionals with specific skills in privacy issues.

About (ISC)²® and the (ISC)² Foundation

(ISC)² is the largest not-for-profit membership body of certified information and software security professionals worldwide, with nearly 100,000 members in more than 135 countries. (ISC)²'s certifications are among the first information technology credentials to meet the stringent requirements of ISO/IEC Standard 17024, a global benchmark for assessing and certifying personnel. (ISC)² also offers education programs and services based on its CBK®, a compendium of information security topics. The (ISC)² Foundation is the charitable trust of (ISC)², aiming to make the cyber world a safer place for everyone with community education, scholarships and industry research like the (ISC)² Global Information Security Workforce Study. More information is available at **www.isc2.org** and **www.isc2cares.org**.

About Booz Allen Hamilton

Booz Allen Hamilton is a leading provider of management and technology consulting services to the US government in defense, intelligence, and civil markets, and to major corporations, institutions, and not-for-profit organizations. Booz Allen is headquartered in McLean, Virginia, employs approximately 25,000 people, and had revenue of $5.86 billion for the 12 months ended March 31, 2012. To learn more, visit **www.boozallen.com**. (NYSE: BAH)

About Frost & Sullivan

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies. **www.frost.com**