FROST & SULLIVAN

50 Years of Growth, Innovation and Leadership

The 2013 (ISC)^2 Global Information Security Workforce Study

A Frost & Sullivan Market Study in Partnership with:

(ISC)^2®

Booz | Allen | Hamilton

strategy and technology consultants

Prepared by
Michael Suby
Global Program Director
Information Security

www.frost.com

CONTENTS

EXECUTIVE SUMMARY

The information security profession, in addition to being a large and growing field, is a barometer of economic health and the changing nature of how business is being conducted. Information security professionals are critical guardians in the protection of networked operations and informational assets. Growth in this profession is a testament to the need for their expertise and also a signal that global economic activity is advancing. Furthermore, changes in information technology (IT) and evolving IT norms on how, when, and where business operations occur—such as BYOD, cloud computing, and social media—remind us that information security professionals must be highly adaptable in learning and applying new skills, technologies, and procedures in order to manage a dynamic range of risks. Not to be overlooked, hackers, attackers, and other threatening entities are also advancing and evolving. Change and complexity in IT and IT norms represent new opportunities for them to succeed in their nefarious pursuits. Consequently, information security professionals have no downtime; there are always new risk management challenges to address.

It is against this backdrop that (ISC)^2, in partnership with Booz Allen Hamilton, with the assistance of Frost & Sullivan, conducted its sixth bi-annual worldwide survey of information security professionals.[1] 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. In addition to producing a rich profile of this profession and its dedication to continuous training and education, this year's survey intensified its focus on the risk and response to BYOD, cloud computing, and social media. Secure software development, touched on lightly in previous surveys, also garnered expanded focus in the 2013 survey. This was done in recognition that software applications are increasingly under attack. Without a corresponding response by security professionals and the technology vendors that support them, this "soft" underbelly of business and governmental entities has and will continue to be exposed with serious consequences—data breaches, disrupted operations, lost business, brand damage, and regulatory fines. **Secure software development, more than any other discipline, is where the largest gap between risk and response attention by the information security profession exists.** Other notable survey findings include:

- **Information security is a stable and growing profession** – Information security professionals are very stable in their employment; more than 80 percent had no change in employer or employment in the past year, and the number of professionals is projected to continuously grow more than 11 percent annually over the next five years.

- **(ISC)^2 membership and location drive higher salaries** – The salary gap between (ISC)^2 members and non-members is widening. Comparatively on a regional basis, 79 percent of information security professionals in developed countries in the Americas have average salaries of US$80,000 or more, whereas only 12 percent of respondents located in APAC developing countries do.

[1] Founded in 1989, (ISC)$^{2®}$ is a not-for-profit global operating organization dedicated to providing education, certification, and peer-networking opportunities for information security professionals throughout their careers.

- **Even with past annual growth in the double-digits, workforce shortages persist** – Fifty-six percent of respondents believe there is a workforce shortage, compared to two percent that believe there is a surplus. The impact of shortage is the greatest on the existing workforce.

- **Knowledge and certification of knowledge weigh heavily in job placement and advancement** – Broad understanding of the security field was the #1 factor in contributing to career success; followed by communication skills. Nearly 70 percent view certification as a reliable indicator of competency.

- **Application vulnerabilities rank the highest in security concern** – Malware and mobile device are close seconds. Mitigating the risk from these and other security concerns to the organization's reputation is the highest priority.

- **While attack remediation is anticipated to be rapid, security incident preparedness is exhibiting signs of strain** – Twenty-eight percent believe their organizations can remediate from a targeted attack within one day. Yet, with regard to being prepared for a security incident, a doubling of the percentage of 2013 survey respondents believe their preparedness has worsened compared to the respondents in the 2011 survey.

- **Information security professionals trump products in securing infrastructure effectiveness** – In a ranking of importance in securing infrastructure, software and hardware solutions rank behind the effectiveness of information security professionals.

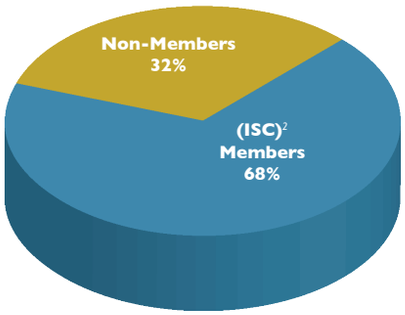
- **Security concern is high for BYOD and cloud computing** – Protecting sensitive information contributes to the security concern noted in both of these IT trends. Security concern with social media is significantly lower than in 2011 as organizations leverage existing security technologies and policy mechanisms to manage this communication channel.

- **New skills, deepening knowledge, and a wider range of technologies needed** – A multi-disciplinary approach is required to address the risks in BYOD and cloud computing. With cloud computing, organizations balance the type of cloud environment with their level of acceptable risk and ability to control risk. For example, with security concern regarding cloud computing being high, private clouds, where the customer has greater control in security risk management, are chosen more frequently than public clouds.

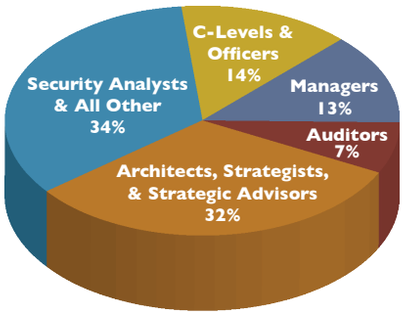
SURVEY OBJECTIVE AND METHODOLOGY

The 2013 Global Information Security Workforce Study (GISWS) was conducted in September-December of 2012 through a Web-based survey, approximately 25 minutes in length. The study's objective is to gauge the opinions of information security professionals regarding trends and issues affecting their profession and careers. Designed to capture expansive viewpoints and produce statistically significant results, a total of 12,396 surveys of qualified information security professionals were collected. The diversity of survey respondents is reflected in the survey respondent profiles shown on the next page.

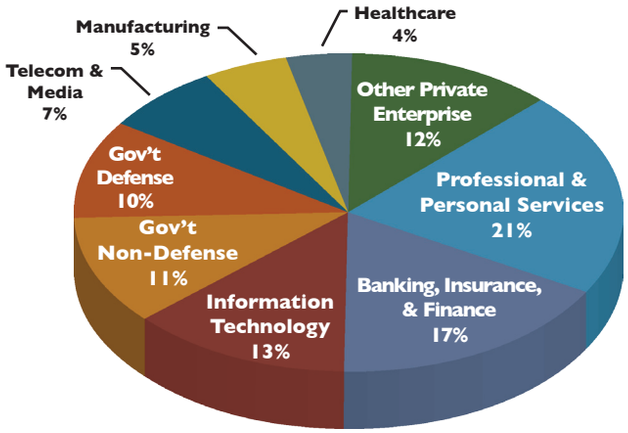
Respondents by Membership



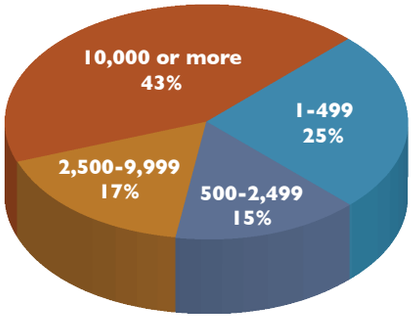
Respondents by Job Title



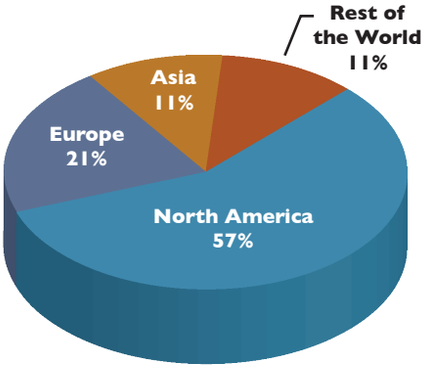
Respondents by Industry Vertical



Respondents by Company Size (Number of Employees)

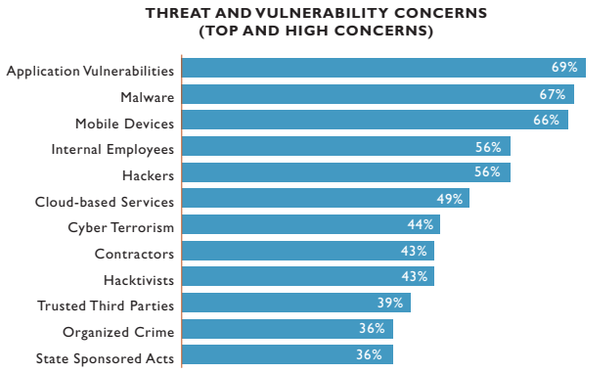


Respondents by Region



SECURITY THREATS AND VULNERABILITIES, IMPLICATIONS AND STATE OF READINESS

As reported in previous GISWS surveys, there is no lack of diversity in the threats and vulnerabilities information security professionals are tackling—and concerned about. All of the 12 threats and vulnerabilities presented in the survey were selected as top or high concerns for 36 percent or more of the survey respondents. At the top of the list, application vulnerabilities, malware, and mobile devices were each identified as a top or high concern by two-thirds or more of the respondents.



Greater examination of Bring Your Own Device (BYOD), including mobile devices, cloud computing, and social media, and their security implications and how information security professionals are responding, is included later in this paper. Secure software development, the upfront means to lessen application vulnerabilities, will also be examined later in this paper.

Focusing deeper into the responses on threats and vulnerabilities reveals that concern severity varies.

- **Some perspectives change over time** – Comparing this year's survey to the 2011 results, the level of concern is fairly stable. However, there was a notable increase in cloud-based services. Compared to the 49 percent of respondents that view cloud-based services as either a top or high security concern in the 2013 survey, 43 percent viewed it as a top or high security concern in the 2011 survey. We believe this increase follows the increased adoption of cloud-based services over the two-year period since the last survey, combined with the resilient security concerns, real and perceived, associated with cloud-based services.

- **C-levels and officers rated nearly all threat and vulnerability categories higher than respondents in other job titles** – This was most notable in application vulnerabilities and mobile device security. Top or high concern was selected by 72 percent of C-levels and officers for application vulnerabilities and 70 percent for mobile devices.

- **Size and anxiety is correlated** – In all threat and vulnerability categories, the average level of concern increased as company size increased. Perhaps the bigger the company is, the more resources it devotes to examining these threats and through that examination, gains a more comprehensive and realistic appreciation of risk and risk implications. Also,

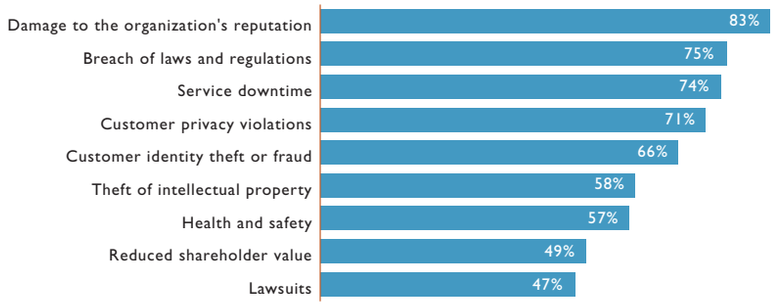
from the "greatest gain for the effort mentality," larger companies represent more lucrative targets for attackers and hackers, thus contributing to a higher level of concern among large company respondents.

- **Vertical equates to variability** – The nature of a company's business and operations also has implications on being a target and with that, variation in concern. No surprise, respondents in the banking, insurance, and finance verticals, with their possession and use of valuable and exploitable personally identifiable and financial information, view the threats posed by hackers, hacktivists, and organized crime higher than the majority of other verticals. Government respondents, also not a surprise, view the threat of state-sponsored acts and cyber terrorism as a greater security concern (i.e., choosing top or high concern) over private enterprises by more than 20 percentage points in each of these threat categories.

- **Developing countries express higher level of concern** – Survey respondents located in developing countries state a higher level of concern for a majority of the threat and vulnerability categories versus respondents in developed countries. Directly contributing to this is that information security investments in developing countries are historically less than the global average. This is reflected in the lower level of security certifications in developing versus developed countries. For example, with the most popular certification chosen by survey respondents—Certified Information Systems Security Professional (CISSP®)—only 42 percent of the survey respondents located in developing countries (members and non-members combined) had acquired and maintained this certification, versus 71 percent of respondents located in developed countries.[2]

Threats and vulnerabilities have implications—attackers are successful and vulnerabilities are exploited. To that point, the survey asked respondents to rank their organizations' priorities: In other words, what needs to be avoided? As shown, damage to the organization's reputation, breach of laws and regulations, and service downtime represent the top three to-be-avoided outcomes. Also noteworthy is the high percentage of top-priority selections. For example, 49 percent of all survey respondents rated damage to the organization's reputation as a top priority. In fact, five of the nine categories received a top-priority rating by more than one-third of the survey respondents. **Conclusion: the "protect and secure" activities of information security professionals are strongly aligned with many high priorities of their organizations.**

ORGANIZATIONS' PRIORITIES (TOP AND HIGH)



Perhaps an indication of information security professionals' improving ability to allay a subset of outcomes, the percent of respondents in the 2013 survey selecting top or high concern for service downtime, customer privacy violations, theft of intellectual property, and lawsuits was down 3-5 percentage points from the 2011 survey for these categories. These reductions notwithstanding, these categories remain high priority.

Notable variation in priority ratings among job titles, company sizes, and verticals are:

- **Auditors' aim is clear** – In keeping with the role of auditor, survey respondents that chose this job title prioritize breach of laws and regulations higher than all other job titles. Also aligned with their roles, managers and security analysts placed a higher priority on service downtime than the other job titles.

- **Priority rises with company size** – Like security concerns, priority ratings rose with company size.

- **Top priority varies among verticals, logically** – Sixty-three percent of banking, insurance, and finance respondents selected damage to the organization's reputation as top priority. In healthcare, 59 percent chose customer privacy violations as top priority. Fifty-seven percent of construction respondents chose health and safety as a top priority, and 50 percent of telecom & media respondents view service downtime as top priority.

With a diversity of threats and vulnerabilities to be concerned with and the need to avoid a range of undesirable outcomes, it is logical to ask about preparedness. In a repeat of the 2011 survey, the 2013 survey requested the respondents judge their change in readiness relative to 12 months earlier (perform better, worse, or same). The results for both surveys are summarized in the following table.

	Percent of Respondent Performance Relative to 12 months Earlier		
	Better	**Worse**	**Same**
Being prepared for a security incident	2013 survey: **41%**	2013 survey: **6%**	2013 survey: 53%
	2011 survey: **55%**	2011 survey: **3%**	2011 survey: 43%
Discovering a security breach	2013 survey: **40%**	2013 survey: **6%**	2013 survey: 54%
	2011 survey: **50%**	2011 survey: **3%**	2011 survey: 47%
Recovering from a security incident	2013 survey: **39%**	2013 survey: **6%**	2013 survey: 55%
	2011 survey: **49%**	2011 survey: **3%**	2011 survey: 48%

While the majority of respondents believe that their organizations would perform better or the same relative to 12 months earlier, there was a 10-point or more decline in the percent of respondents believing they would perform better in the 2013 survey compared to the 2011 survey. Not as significant, but equally disconcerting about improvement in the state

[2] The percent of survey respondents with certifications other than CISSP (e.g., ITIL, CISA, and Security+) was materially lower, and the difference between developed and developing countries was less (10 percentage points difference or less).

of readiness, twice the percentage of respondents in the 2013 survey view their readiness has worsened in the past year as did respondents in the 2011 survey. **As an indication that membership really matters, the survey-over-survey decline in the percent of respondents selecting "better," and increase in selecting "worse," was not as profound with member respondents compared to non-member respondents.**

Other noteworthy observations from the 2013 survey on these readiness categories include:

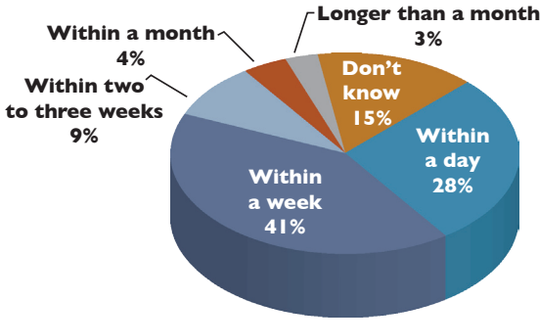
- **C-levels and the rank-and-file differ** – Respondents with C-level and officer job titles were decidedly more optimistic on readiness; they chose "perform better" by a greater percentage than respondents in all other job title categories.

- **Largest companies more optimistic** – In all three categories of readiness, a greater percentage of the largest companies (10,000 employees or more) viewed that their readiness had improved versus smaller companies. Reflecting the correlation between readiness and training, and smaller companies being less optimistic on their readiness than large companies, a greater percent of survey respondents in companies with 2,500 or fewer employees than larger companies indicated spending on training and education increased in the past 12 months and is expected to increase over the next 12 months as well.

- **Battle-tested banking, finance, and insurance verticals confident they are turning the tide** – Respondents in these industries chose "perform better" to a greater extent than all other verticals in all three categories. Conversely, the respondents in the less battle-tested utilities vertical chose "perform worse" to a greater extent than any other vertical.

Another survey question focused on readiness is how quickly damage from a targeted attack would be remediated. Slightly more than two-thirds of the respondents project that they could remediate the damage from a targeted attack within a week or less. Yet, there is also a material portion of the respondents that are unsure how long damage remediation might take.

Time to Remediate from a Targeted Attack



- **As typical, C-levels voiced greater assurance on their organizations' readiness** – C-levels and officers chose "within one day" or "don't know" less than respondents with job titles farther down the organizational structure—31 percent and 10 percent, respectively.

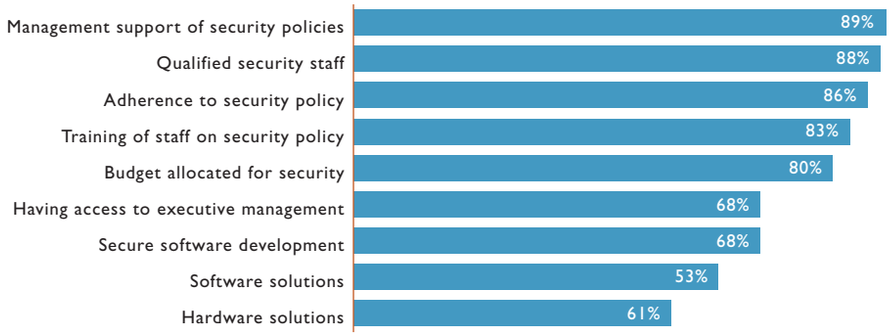
- **Smallness advantage** – With a less diverse and smaller spread of operations, 31 percent of small companies (less than 500 employees) believe they can remediate in one day and 44 percent within a week. This is a faster expectation than very large companies (10,000 or more employees)—28 percent and 39 percent, respectively. Also, respondents in very large organizations chose "don't know" to a greater extent (18 percent) than small companies (12 percent).

- **Experience advantage** – Banking, insurance, and finance verticals, plus the info tech vertical, believe they can respond faster than other industries; 34 percent and 32 percent of respondents in those verticals, respectively, predicted within one day to remediate. Potentially due to highly distributed operations, respondents in the retail & wholesale and construction verticals chose "don't know" at higher levels—19 percent and 20 percent, respectively. Potentially, a lack of experience in past remediation efforts influenced 20 percent of respondents in the utilities vertical to choose "don't know."

PEOPLE ARE A KEY TOOL IN INFORMATION SECURITY

With the pervasiveness, diversity, and evolution in security threats, information security professionals use an assortment of tools. **Top of the list are human aspects: management support, qualified staff, and policy adherence, with half or greater of respondents choosing very important for each.** The next four categories also have a human aspect. Security software and hardware are materially farther down the list of essential tools in effective security; confirming the viewpoint that the effectiveness of security technologies is maximized only when the trained human element is actively incorporated.

IMPORTANCE IN SECURING INFRASTRUCTURE (VERY IMPORTANT AND IMPORTANT)



Other observations include:

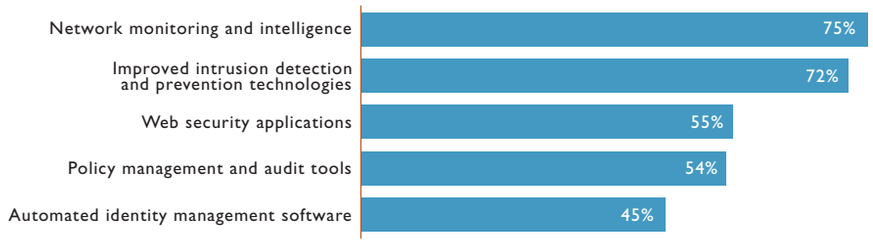
- Compared to the 2011 survey, the average importance ratings were essentially unchanged in the 2013 survey.

- C-levels and officers indicated a higher importance on access to executives than respondents in other job titles, indicating that these respondents believe their greatest influence occurs at their peer level.

- As organization size increases, importance on human assets increases, whereas the importance of hardware and software is even across company sizes.
- Across industry verticals, respondents in the government place higher importance on hardware and software solutions than the companies in the private sector.
- **Secure software development is viewed as more important by banking, finance, and insurance; info tech; retail and wholesale; and telecom and media verticals.**

Concentrating on select security technologies that provide significant improvement in system and network security (those that garnered more than 10 percent of respondent selection), two technologies were highlighted by the survey respondents for their capabilities: network monitoring & intelligence, and intrusion detection & prevention.

TECHNOLOGIES THAT SIGNIFICANTLY IMPROVE SYSTEM AND NETWORK SECURITY



Other perspectives are:

- Aside from the technologies shown, no other selectable technology in the survey gained more than one percent of survey respondents' votes. Other selectable technologies included: authentication, network access control (NAC), and security incident and event monitoring (SIEM).
- There was no tangible difference in selection frequency by company size or job title.
- Owing to the public-facing attribute of their businesses, Web security applications had the greatest frequency of votes by the banking, finance, and insurance; education; info tech; and retail and wholesale verticals. Healthcare respondents selected policy management and auditing tools in greater numbers than respondents in other verticals.

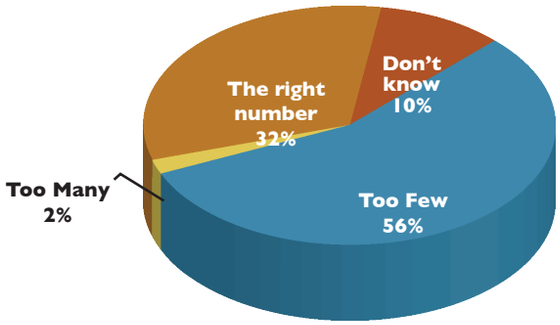
NEED AND BUDGET FOR THE RIGHT INFORMATION SECURITY PROFESSIONALS

With security staff viewed as critical in importance, it is equally important to understand the acuteness of need, organizations' ability to fund staff expansion and improvement, and the sought-after attributes of information security professionals.

The need is present

- **Very few respondents view their security organizations as being over-staffed.** Nearly one-third of respondents believe they have the right number of staff, but more than 50 percent believe staff expansion is justified.
- The good news is that two-thirds of C-levels, those with the greatest budgetary influence, view their security organizations as being too few in numbers.
- More midsize companies' (500-2,499 employees) respondents view their organizations as understaffed versus smaller and larger size companies.
- Across industries, a greater percentage of respondents in education, healthcare, manufacturing, and retail & wholesale verticals believe they are understaffed.

Does Your Organization Currently Have the Right Number of Information Security Workers?



The strain of understaffing is felt greatest on the existing security workforce—greater than the overall organization, security breaches, and customers.

The reasons for an inability to bridge the need for additional information security workers are fueled by three factors: business conditions, executives not fully understanding the need, and an inability to locate appropriate information security professionals. Other reasons provided by respondents—such as economy, lack of funding or budget, and staffing cuts or layoffs—were volunteered by one percent or less of the respondents. Across verticals, respondents in info tech view an inability to find qualify personnel as a larger impediment to staffing than other verticals. When asked which job title experienced the greatest workforce shortage, security analyst (chosen by 47 percent of respondents) topped the list, followed by security engineering-planning and design (32 percent), and security auditor (31 percent).

IMPACT OF INFORMATION SECURITY WORKFORCE SHORTAGES (VERY GREAT AND GREAT IMPACTS)

Budget availability to increase spending is strong

An increase in spending is predicted by nearly one-third of survey respondents in personnel, training and education, and hardware and software. Slightly more than 10 percent, however, predict a decline. This decline is more prevalent in government (approximately 19 percent of respondents predicting declines) versus private sector (approximately 10 percent of respondents predicting declines). More than any other private sector vertical, 35 percent of respondents in the info tech vertical predict spending increases.

How will information security spending change over the next 12 months?	Percent of Respondents		
	Increase	Decrease	Same
Information security personnel	30%	12%	59%
Training and education	28%	13%	60%
Hardware and software	32%	11%	57%

Slightly more than one-third (34 percent) of C-levels expect their spending on personnel to increase over the next 12 months. Also, 31 percent of C-levels predict increased spending on education and training.

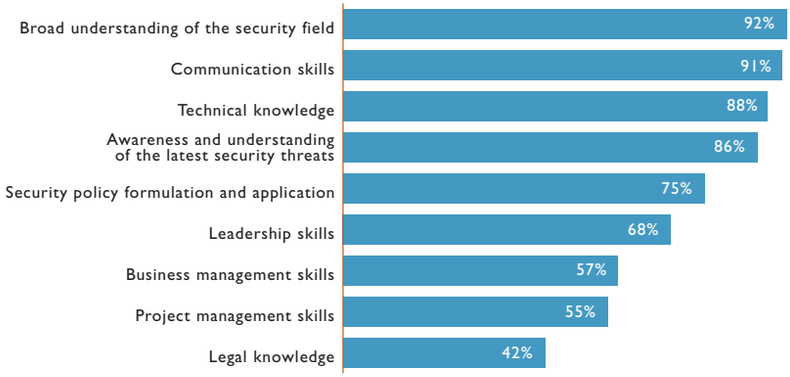
Sought-after attributes in information security professionals

When examining the sought-after attributes of information security professionals, it is not just the skills that are important. Confirmation of those skills (i.e., certification) and professionals' engagement in peer groups (i.e., affiliations) are also essential. The importance attached to each is examined in this section.

Skills

Across the entire survey, broad understanding of the security field was on top in terms of importance, followed by communication skills. Technical knowledge, awareness and understanding of the latest security threats round out the top four.

SUCCESS FACTORS OF INFORMATION SECURITY PROFESSIONALS (IMPORTANT AND VERY IMPORTANT)



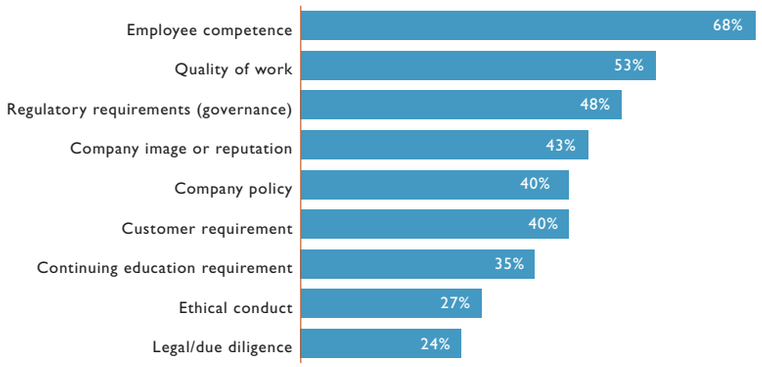
Respondents in the banking, finance, and insurance verticals place a higher emphasis on the importance of broad understanding than other verticals. Info tech and government-defense place higher importance on technical knowledge. Healthcare respondents rate communication skills higher in importance.

Certification

Slightly more than 46 percent of all survey respondents indicated that their organizations require certification, and among those respondents, 50 percent of member and 39 percent of non-member indicate certification is a requirement. Government-defense is most emphatic on this point; 84 percent state certification is required, and a distant, but still high, second is info tech at 47 percent.

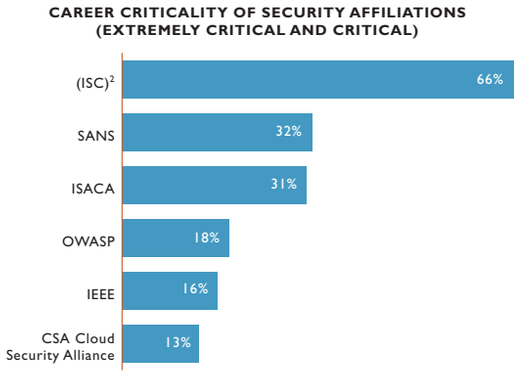
While regulations are a primary driver for certification in government-defense, that is an anomaly. The private sector overwhelmingly (74 percent) views certification as an indicator of competency. The correlated quality of work was the second highest reason.

REASONS FOR REQUIRING INFORMATION SECURITY CERTIFICATIONS



Affiliations

When asked about affiliations that matter most in career development and resiliency, (ISC)^2 was rated the highest, no surprise by (ISC)^2 members (74 percent chose extremely critical or critical), but the same is true with non-(ISC)^2 members (51 percent chose extremely critical or critical). SANS and ISACA were ranked the next two in importance for each survey group.

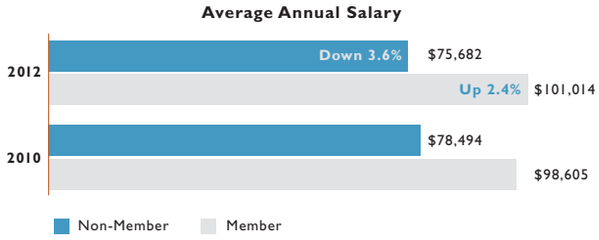


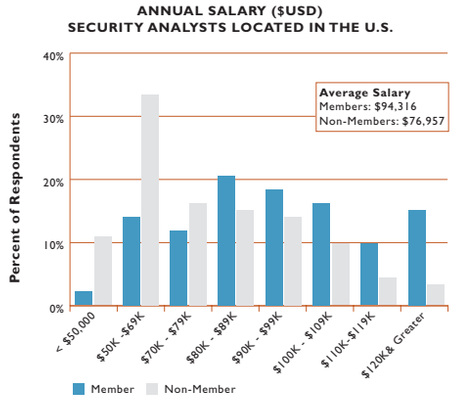
INFORMATION SECURITY IS A REWARDING AND RESILIENT PROFESSION

The importance of the information security profession has been clearly articulated in this survey by the respondents, which does include bias as they have chosen this career. To gain a more unbiased confirmation of the importance of this profession, the survey asked respondents to weigh in on the uniform measuring sticks of all careers: salary, change in salary, and job stability.

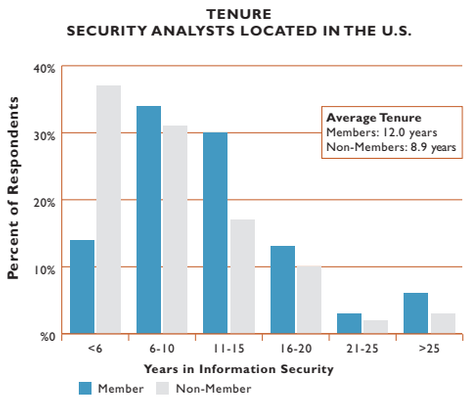
In terms of salary, the average annual salary across all survey respondents is US$92,835. As expected, C-levels and officers reported the highest average annual salary at US$106,151. The respondents in government-defense and healthcare reported the highest average annual salaries at US$101,246 and US$98,037, respectively.

In comparing average annual salaries for members and non-members between the 2013 and 2011 surveys, the member average salary is higher, and the salary gap between members and non-members is widening. Recognizing that many factors influence salary—job title, location, security certifications, and tenure—a narrower examination on salary is appropriate. To gain the greatest confidence possible in salary comparisons with the survey data, we selected the job title and location with the greatest number of respondents: security analyst located in the U.S. **As displayed, U.S.-based security analysts that are (ISC)^2 members, on average, have a higher salary—23 percent greater than U.S.-based security analysts that are non-members. (see chart on next page)**





Part of the reason for the higher salaries is tenure; (ISC)[2] security analyst members located in the U.S. averaged 35 percent longer careers than non-members. And, as shown, tenure distribution is skewed to the right for members. The conclusion from these two comparison charts between members and non-members is that for one job title in one country, member professionals sustain a longer career and receive higher rewards (i.e., pay). We project that a similar finding would be confirmed with other job titles and locations, provided there is a sufficient number of respondents to produce statistically significant comparisons.



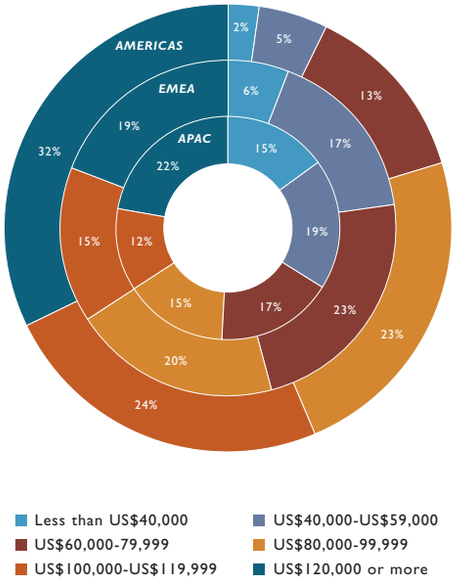
Salaries of information security professionals have been and continue to be on the rise. In the table on the next page are the self-reported salary changes recorded in the 2013 and 2011 surveys.

Salary change in current year?	Percent of Respondents	
	2013 Survey	2011 Survey
Yes, an increase up to 5%	40%	39%
Yes, an increase between 5% and 10%	12%	14%
Yes, an increase of over 10%	8%	9%
No change in salary or benefits	36%	34%
Received a salary or benefit reduction	4%	4%

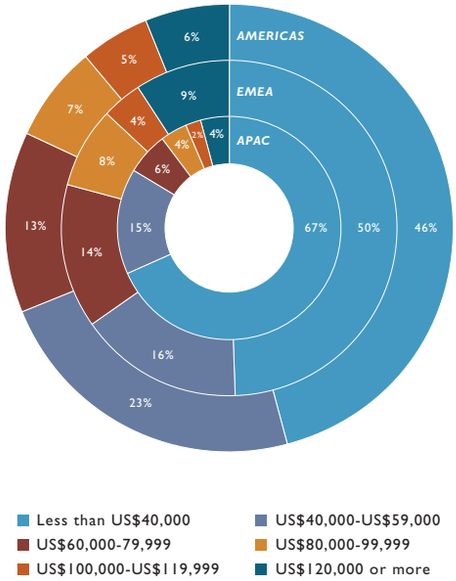
There are no notable differences in this distribution of salary changes by either job title or company size in the 2013 survey. There are, however, differences among the verticals. These differences provide an indication of which verticals are using salary to retain and reward security professionals more than other verticals. For example, 11 percent of respondents in the info tech vertical reported receiving a salary increase of more than 10 percent in 2012. Conversely, education and government are not rewarding their information security professionals to the same degree. Forty-four percent and six percent of education respondents reported no change or reduction in salary, respectively, in 2012. For respondents in government, the results are similar: 45 percent reported no change and five percent reported a salary reduction.

Another notable comparison in salary differences is across region and developmental stage of countries (i.e., developed versus developing). The following two charts display salary range distribution, first for respondents in developed countries and second in developing countries.

DEVELOPED COUNTRIES



DEVELOPING COUNTRIES



Less than US$40,000 | US$40,000-US$59,000 | US$60,000-79,999 | US$80,000-99,999 | US$100,000-US$119,999 | US$120,000 or more

These tables on the next page highlight the degree of differences in salary distribution across geographies. **Notable, a far greater percent of information security professionals located in the Americas command higher salaries than professionals in other regions.**

Region	Percent of Respondents with Annual Salaries of US$80,000 or More	
	In Developed Countries	In Developing Countries
Americas	79%	18%
EMEA	54%	21%
APAC	49%	12%

Reversing the table contents and focusing on annual salaries of less than US$40,000, information security professionals located in developing APAC countries have the highest proportional representation.

Region	Percent of Respondents with Annual Salaries of Less than US$40,000	
	In Developed Countries	In Developing Countries
Americas	2%	46%
EMEA	6%	50%
APAC	15%	67%

Regarding employment stability, the information security profession is highly resilient. **As shown in the following table, only three percent of respondents reported an employer change due to layoff or termination consistently in the two surveys.**

Change in employer or employment status in current year?	Percent of Respondents	
	2013 Survey	2011 Survey
No change in employer or employment status	83%	82%
Yes, changed employer while still employed	11%	12%
Yes, changed employer due to layoff or termination	3%	3%
Yes, became self-employed	2%	2%
Yes, became an employee from being self-employed	1%	1%

In terms of the long-term employment picture for information security professionals, **Frost & Sullivan predicts double-digit, year-over-year percentage increases over the next five years.**[3] In 2013, Frost & Sullivan predicts global employment of information security professionals to increase 332,000, ending the year at 3.2 million.

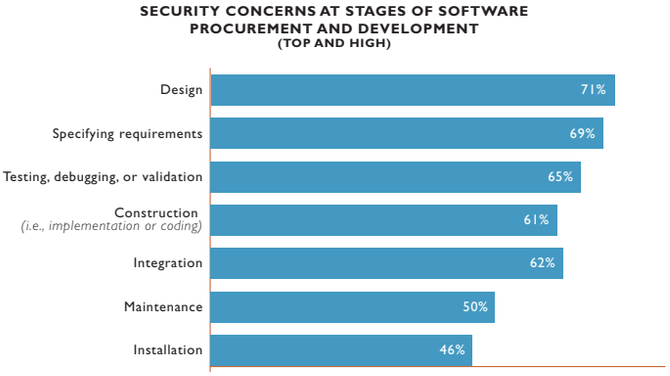
Thousands	2010	2011	2012	2013	2014	2015	2016	2017	2012-2017 CAGR
Americas	921	1,045	1,181	1,331	1,495	1,673	1,867	2,081	12.0%
EMEA	617	704	797	892	995	1,108	1,230	1,363	11.3%
APAC	748	817	894	981	1,079	1,191	1,320	1,463	10.4%
Total	2,283	2,566	2,872	3,204	3,568	3,972	4,416	4,908	11.3%

[3] This table reflects Frost & Sullivan's best estimate and projection of 2010 - 2017 employment of information security professionals. Professionals in both managerial and operational roles are included. Data from a variety of sources, including credible secondary sources and internal research was incorporated. This year's forecast is slightly less than the employment forecast developed two years ago due to refinement in the forecasting methodology. Greater emphasis was placed on correlation analysis with Frost & Sullivan's sizing of global market expenditures on security products and services, and with regional variations contained in the survey data.

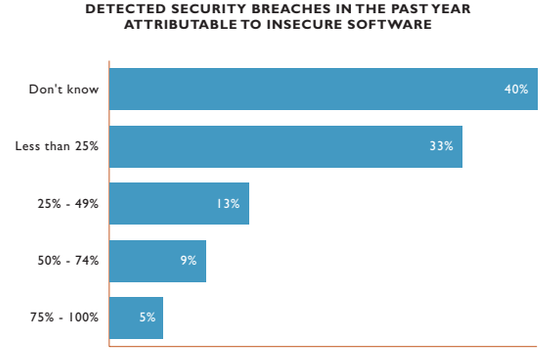
SECURE SOFTWARE DEVELOPMENT: ESSENTIAL BUT UNDER-SUPPORTED

Application vulnerabilities was the number one security concern for survey respondents. **Closer examination reveals that the secure software development concern increases with company size, perhaps correlated with the greater amounts of software development in large companies versus smaller companies that rely heavily on commercial applications. Also, the importance of secure software development was rated above software and hardware solutions in securing the organization's infrastructure.** Here, too, there is variance associated with company size. In particular, as company size increases, the importance of secure software development relative to the importance of software and hardware solutions also increases.

Recognizing that software procurement and development involves multiple phases, the level of security concern may fluctuate among these steps. According to the survey respondents, this is true but within a fairly narrow range in the pre-installation steps.

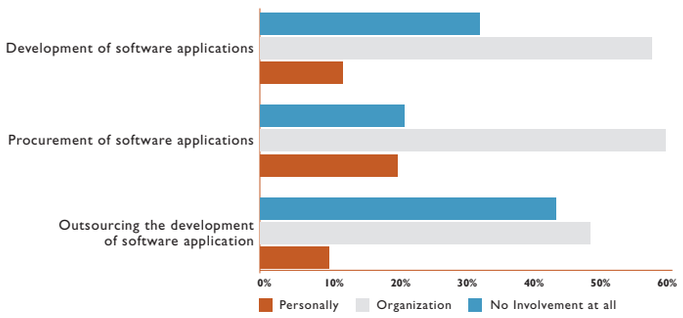


The risk implications of these concerns are most notable in the proportion of detected security breaches attributed to insecure software. According to survey respondents, insecure software was a contributor in approximately one-third of the 60 percent of detected security breaches. In the other 40 percent of detected breaches, insecure software's role was uncertain either because post-breach forensics were inconclusive, or the survey respondents were not privy to the forensics. Regardless of this uncertainty, along with insecure software's unquantifiable attribution in undetected breaches, information security professionals are certain that their concerns regarding insecure software are justified.



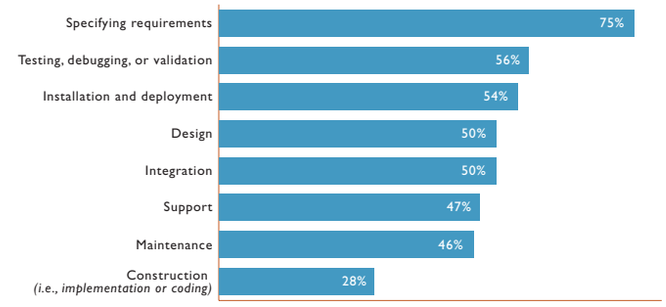
The next question is, what is being done to mitigate or resolve the risk of insecure software? This mitigation begins by being involved in software development, procurement, and outsourcing. According to survey respondents, approximately 50 percent state that someone other than themselves from their security organizations is engaged in software development, procurement, and outsourcing. **Not so promising of information security professionals' involvement is the substantially lower percent personally involved in software development (12 percent), procurement (20 percent), and outsourcing (10 percent).** Considering the size and comprehensive reach of the GISWS, and the high level of concern and attributed risk assigned to insecure software, this survey observation is one signal that a material gap exists between risk and response.

INVOLVEMENT IN SOFTWARE DEVELOPMENT, PROCUREMENT AND OUTSOURCING



The phases of software procurement and development that this subset of information security professionals is engaged in are diverse. **The most common phase of personal involvement is specifying requirements (75 percent). Involvement in stages that confirm that these requirements are meeting their objectives drops off considerably.** This, too, is a signal of a gap between risk and response by information security professionals and their organizations.

INVOLVEMENT IN SOFTWARE PROCUREMENT AND DEVELOPMENT STAGES



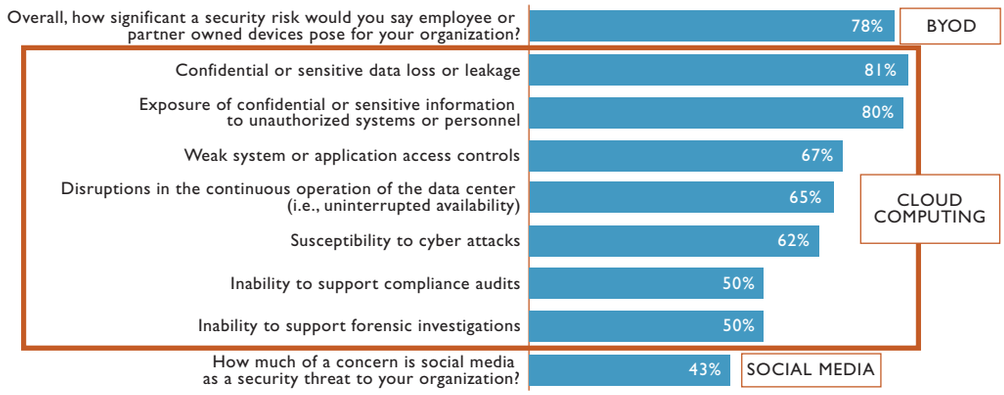
As reported previously in this study, information security professionals, members, and non-members, view acquiring new skills and certification as very important. **Earning certifications most applicable to secure software, however, is hardly a blip on the list of certifications survey respondents claim.** For example, only one percent of surveyed information security professionals claim to have acquired the Certified Secure Software Lifecycle Professional (CSSLP®) certification. This is also a signal that the gap between insecure software risk and response is real.

The conclusion is apparent: unless software and information security professionals' involvement is deepened in secure software development, procurement, and outsourcing; and training and education permeates the ranks of software development functions, the risks associated with insecure software will remain. **Furthermore, deepening engagements in software development cannot occur in isolation or be the exclusive responsibility of the information security workforce. Other relevant functional groups—software developers, application owners, and the quality assurance and testing teams—must internalize secure software development best practices and engage, as standard operating procedure, with information security professionals.** While expertise in the information security discipline varies across groups, all groups must be responsible in order for the risk and consequences of insecure software to decrease.

SECURITY IMPLICATIONS OF BYOD, CLOUD COMPUTING, AND SOCIAL MEDIA

In this section, we zero in on the survey responses to three prominent IT trends: BYOD, cloud computing, and social media. Each is unique in their security implications and how information security professionals and their organizations are managing risk. For example, assessment of security risk is not uniform. BYOD is the highest overall, followed by cloud computing and social media. We believe that the "it's just happening" and "happening at accelerating speed" with BYOD are forcing organizations to react more than with cloud computing, where adoption and use is more of a managed choice by companies. **Consequently, the risk in BYOD is "cast upon" businesses more so than evaluated and chosen with cloud computing.** Social media is different. While social media, too, has the "cast upon" attribute of BYOD, social media represents more of an evolution in internal and external communication channels than the introduction of a mushrooming range of user-owned and therefore untrusted user devices. As such, companies have experience in managing the risk of unauthorized communications (e.g., when instant messaging and Web-based email became broadly available), with many of the same and existing technologies and procedures to monitor and manage the communication flows. Consequently, the security risk with social media is less than BYOD.

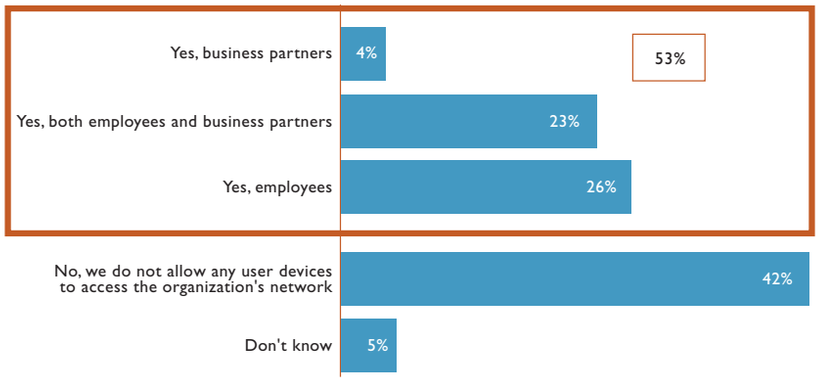
BYOD, CLOUD COMPUTING, AND SOCIAL MEDIA
(TOP 2 ON 5-POINT SCALE OF SECURITY SIGNIFIGANCE OR CONCERN)



BYOD

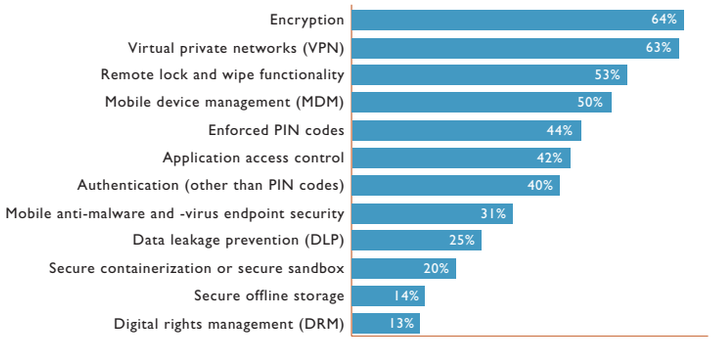
Approval for use of user-owned devices, according to this survey, is more than 50 percent. Differences in allowance do exist, primarily among verticals. For example, 67 percent of respondents in government state user-owned devices are not allowed. In the private sector, 47 percent of respondents in banking, insurance, and finance verticals state user-owned devices are not allowed. **At the other end, education is most permissive, with 86 percent of education respondents claiming user-owned devices (employee and business partners combined) are allowed.**

ALLOW USER-ORIENTED DEVICES (BYOD)



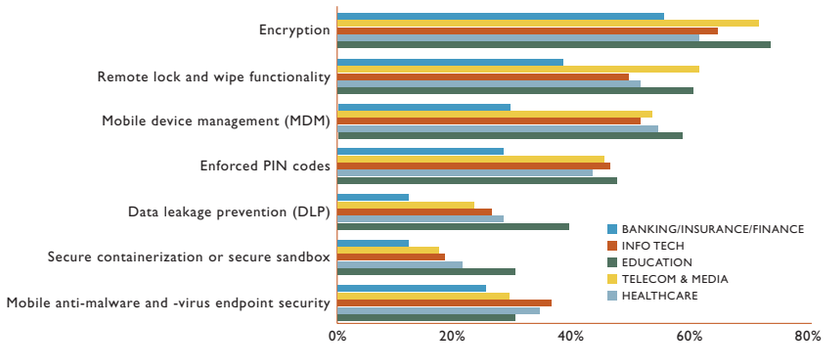
End-user license agreements are one way that companies manage BYOD risk. Fifty-one percent of survey respondents claim agreements are in use. Beyond these agreements, a growing number of security technologies are used. Furthermore, all mobile security technologies listed in the 2011 survey (encryption, remote lock and wipe, MDM, mobile anti-malware, and DRM) had a greater percent of respondents claiming use in 2013. **Also as a sign of expanding security technologies in use are the modest percentages assigned to technologies that were in their commercial infancy in 2011, such as secure containerization or secure sandbox, with 20 percent of respondents stating it is used in the 2013 survey.**

MOBILE DEVICE SECURITY TECHNOLOGIES IN USE



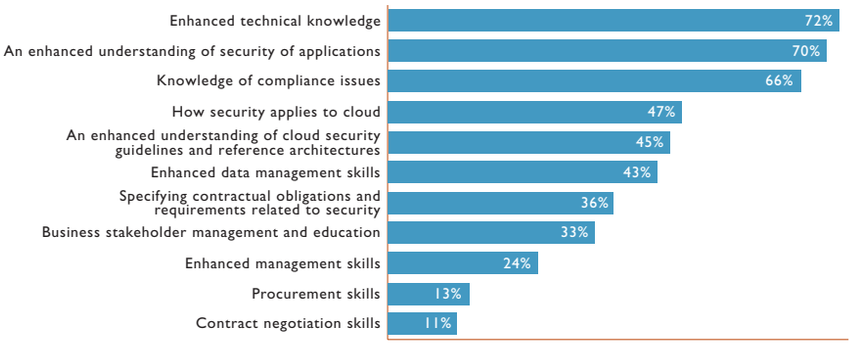
Another interesting perspective revealed in the survey is how mobile security technology use varies among industry verticals. The chart below shows differences for five verticals, including the most permissive allowance of user-owned devices vertical (education) and the most restrictive (banking, insurance, and finance). *Note: Only mobile security technologies that had use differences of 10 percentage points or more are shown.*

DIFFERING MOBILE DEVICES' SECURITY TECHNOLOGIES IN USE AMONG SELECT INDUSTRY VERTICALS



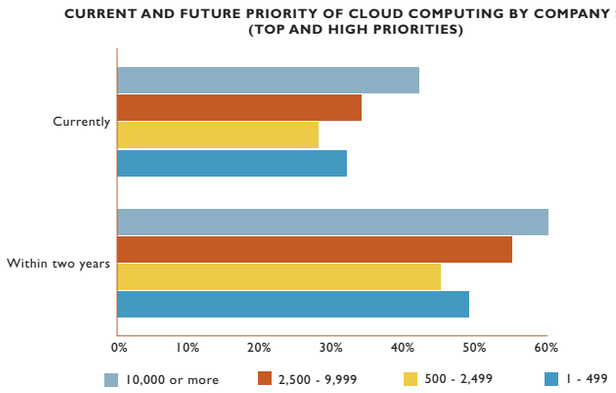
Development of new skills in mobile security and BYOD by information security professionals was noted as required by 74 percent of respondents. This opinion has little variation by company size, job title, or industry vertical. This chart shows which new skills are most required in dealing with mobile security and BYOD.

SKILL REQUIRED IN DEALING WITH MOBILE SECURITY AND BYOD



Cloud Computing

The GISWS confirms the prevailing use of cloud computing is the greatest with large companies (2,500 or more employees). Among industry verticals, the cloud computing priority varies moderately. Respondents in info tech have the highest cloud computing priority; 57 percent chose top- or high-priority cloud computing currently and expect priority to rise to 69 percent in two years. Government respondents express the lowest current and future cloud computing priority ratings (top and high)—26 percent and 45 percent, respectively.

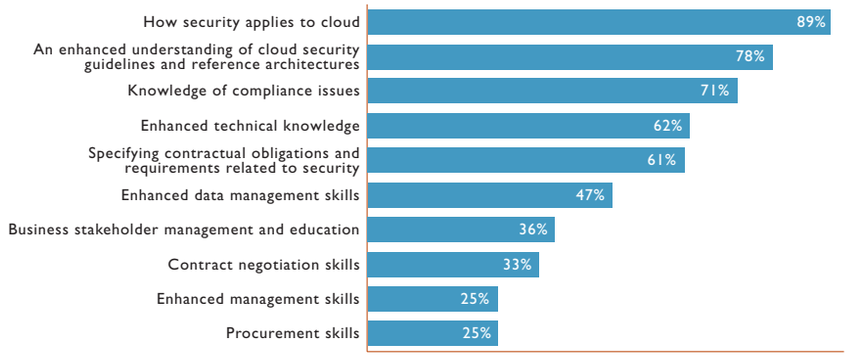


Selection among cloud computing approaches corresponds to the high level of risk currently associated with the cloud. As shown in the table below, private cloud computing services have the greatest proportionate use. With private cloud computing services, the cloud customer retains more control over the cloud infrastructure and how that infrastructure is secured than other approaches.

	Proportionate Use of Cloud Computing Approaches — Current						
	Total Survey	Banking, Insurance & Finance	Education	Healthcare	Info Tech	Telecom & Media	Gov't
Private cloud computing services	38%	41%	37%	38%	34%	37%	46%
Software as a Service	19%	22%	19%	25%	19%	15%	13%
Infrastructure as a Service	11%	11%	7%	8%	12%	13%	11%
Public cloud computing services	11%	8%	16%	10%	11%	12%	9%
Platform as a Service	7%	7%	5%	6%	8%	9%	7%
Hybrid cloud computing services	7%	6%	7%	7%	8%	8%	8%
Community cloud computing services	6%	4%	9%	6%	6%	6%	6%

Similar to mobile security and BYOD, 74 percent of survey respondents believe new skills will be required to manage the risks anticipated with cloud use.

SKILLS REQUIRED IN DEALING WITH CLOUD COMPUTING

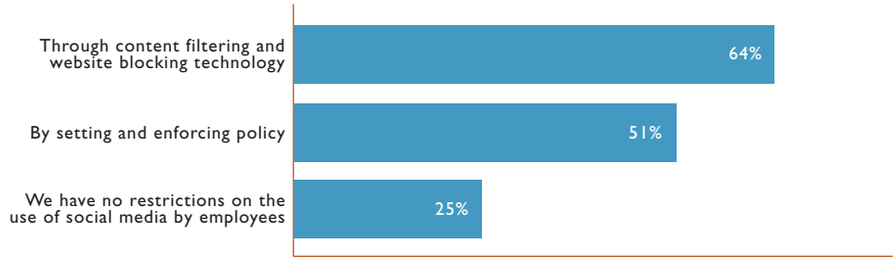


The chart above lists the skills information security professionals believe are needed to manage cloud risks. **The very high percentage of respondents choosing "understanding" skills is indicative that there remains considerable ambiguity regarding cloud-related risks.** Furthermore, with cloud services providers not bound by industry standards or regulations with regard to security practices and procedures, general understanding of potential cloud risks would be incomplete in assessing risk. A thorough understanding of each potential cloud service provider would be required to adequately assess risk across providers.

Social Media

As previously shared, the security concern with social media is less than BYOD and cloud computing. Nevertheless, there is sufficient concern that a majority of information security professionals take action to manage the risk emanating from social media use. The most prominent means to limit access to social media is by using content filtering and website blocking technologies. The prominence of these technologies is greater with larger companies than small. Not surprisingly, higher proportions of medium, large, and very large companies surveyed use this technology for social media access control than small companies. Also as expected, survey respondents in the banking, insurance, and finance verticals expressed greater use (82 percent) of these technologies than any other vertical. **Respondents in the education vertical are the most permissive in social media access; 59 percent state their organizations have no social media restrictions.**

HOW EMPLOYEE ACCESS TO SOCIAL MEDIA IS LIMITED



THE LAST WORD

The professional discipline of information security is complex and requires continuous investment in knowledge, procedures, and technologies. Moreover, the application of information security is the duty of all members of the organization. From a practical perspective, there is a shared need to protect what is important—sensitive information and critical business operations—and a shared responsibility as system users and their devices represent a widely distributed and dynamic field of entry points into public and private networked operations and informational databases. Without organizationally broad awareness and attentiveness to security policies, risk will surely rise and, as a consequence, contribute to sub-optimized effort by information security professionals. More time will be driven to incident response and remediation, and away from proactive building of security practices that meet the organization's risk management objectives and directly contribute to strategic business initiatives (e.g., development and implementation of cutting-edge software applications, mobilizing workforce and operations, and extracting maximum benefits from the evolution in information technologies, such as cloud computing).

For those who have chosen a career in information security, it is a rewarding profession both intellectually and financially. And while skill and knowledge building must never slow down—attackers, hackers, and other cyber threat actors certainly will not—information security professionals must also translate their risk management expertise into organization-wide leadership. Consider if those with the greatest understanding of risk management operate in isolation or, worse, choose to violate security policies. Members of other functional areas in the organization will view information security as an optional responsibility and be equally, if not more, cavalier in their adherence to security policies. Therefore, it is incumbent upon information security professionals to demonstrate security consciousness, and openly and freely engage with members of other departments to show how security is best when practiced together.

Michael P. Suby
VP of Research
Stratecast | Frost & Sullivan
mike.suby@frost.com

(ISC)² would like to acknowledge and thank the following organizations for their participation in the 2013 (ISC)² Global Information Security Workforce Study: Sri Lanka CERT|CC, ISACA, Alderbridge, GFI Software, Reed Exhibitions – Infosecurity Europe, Acumin, CompTIA, Information Security Forum, NASCIO, Security Bsides, IAPP, U Fairfax, Executive Women's Forum, IT Security C&T, SecuMedia, The European Association for e-Identity and Security, BUiM Group for All in the Cloud Asia 2012, ISSA Poland, SANS, ASIS International, IAPP, SEC, RSA, MIS Training Institute, Hashdays, IT Security Pro, Firebrand Training UK, Data Security Council of India (DSCI), Information Security Solutions, and Cast Forum.

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

ABOUT (ISC)²® AND THE (ISC)² FOUNDATION

(ISC)² is the largest not-for-profit membership body of certified information security professionals worldwide, with nearly 90,000 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? Contact Us: Start the Discussion

For information regarding permission, write:
Frost & Sullivan
331 E. Evelyn Ave. Suite 100
Mountain View, CA 94041

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