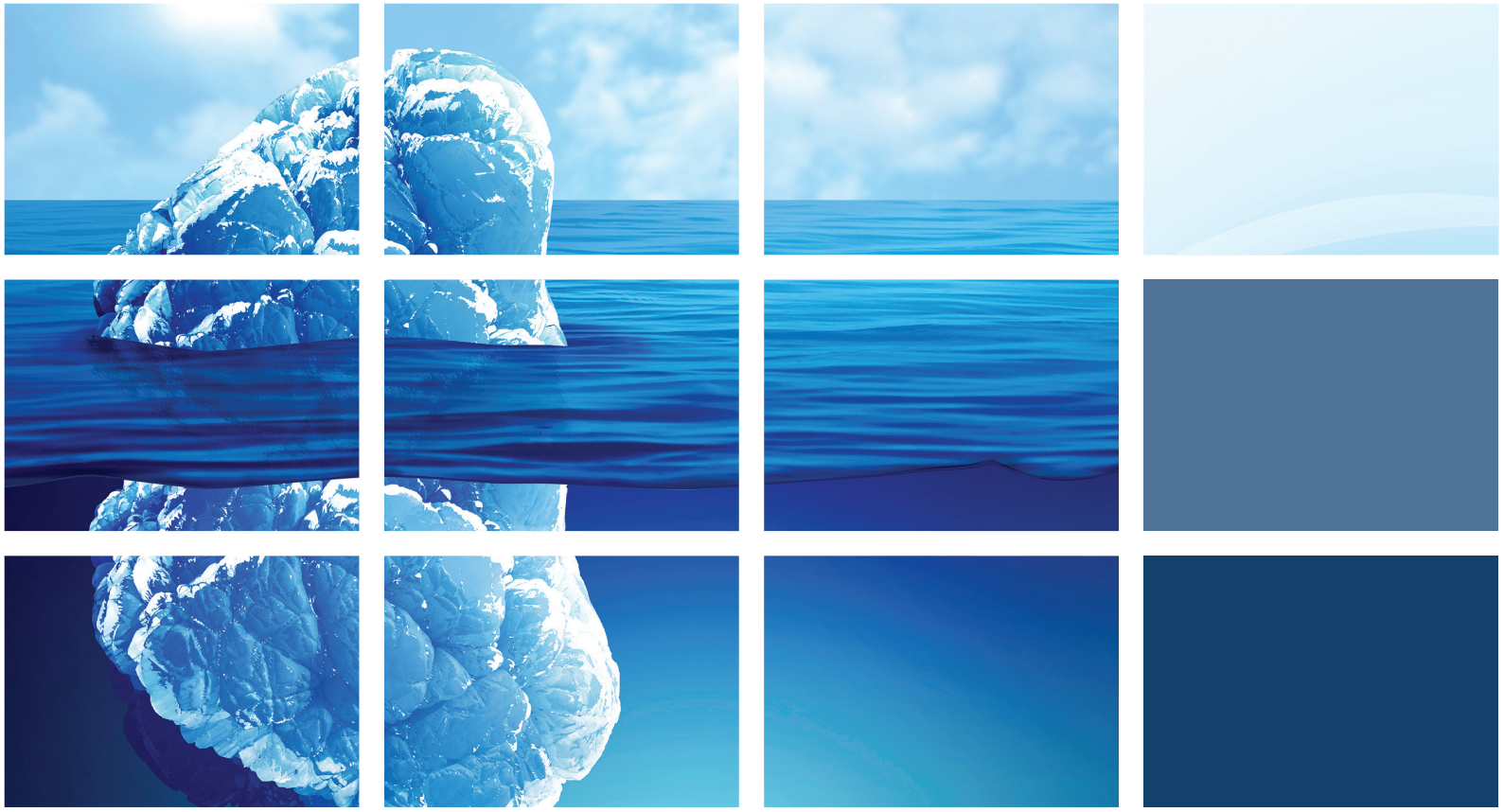


The 2015 (ISC)² Global Information Security Workforce Study

FROST & SULLIVAN

A Frost & Sullivan White Paper

Michael Suby, VP of Research
Frank Dickson, Research Director
Information & Network Security

A Frost & Sullivan Market Study in Partnership with:

(ISC)²®

Booz | Allen | Hamilton
strategy and technology consultants

NRI SECURE TECHNOLOGIES

CYBER 360 A WOMAN-OWNED BUSINESS

contents

EXECUTIVE SUMMARY

The information security workforce shortfall is widening. In this year's survey, 62% of the survey respondents stated that their organizations have too few information security professionals. This compares to 56% in the 2013 survey. Also in a shift from the 2013 survey, the reasons for this hiring shortfall are less about money as more organizations are making the budgets available to hire more personnel. Rather, an insufficient pool of suitable candidates is causing this shortfall. These new observations and others generated from this extensive survey (almost 14,000 respondents globally) allowed Frost & Sullivan, for the first time, to estimate the shortfall in the global information security workforce; which we project will reach 1.5 million in five years. This shortfall is the difference between Frost & Sullivan's projection of the workforce needed to fully address escalating security staffing needs and our workforce projection that accounts for workforce supply constraints (e.g., a tightening labor market among security professionals).

This projected workforce shortfall does not mean hiring will stop. Where possible, organizations will increase their security staffing levels. Again reflecting the reality of a constrained pool of suitable candidates, Frost & Sullivan predicts a global increase of 195,000 information security professionals in the next year; an increase of nearly 6% over 2014. Increased expenditures in training and education are also projected by the survey respondents.

While the ceaseless advancement in variety and sophistication of cyber-threats and a broadening footprint that requires security oversight (e.g., mobile devices, cloud-based services, and the Internet-of-Things) are contributors to rising workforce demand and a workforce with a broader range of qualifications, other contributors are self-inflicted due to decisions organizations make on security priorities. For example, vulnerable software applications continue to be placed into production and end-users continue to be duped by phishing exploits. Even though application vulnerability scanning conducted throughout the software development cycle and periodically in production would mitigate this exposure, this practice is far from routine in the vast majority of organizations. Separately, a security-conscious end-user community would seem to be an essential line of defense, but the survey respondents are showing less confidence in the effectiveness of end-user security training and education.

Signs of strain within security operations due to workforce shortage are materializing. Configuration mistakes and oversights, for example, were identified by the survey respondents as a material concern. Also, remediation time following system or data compromises is steadily getting longer. The net result is that information security professionals are increasingly cornered into a reactionary role of identifying compromises, recovering from mistakes, and addressing security incidents as they occur rather than proactively mitigating the contributing factors.

Confronted with this set of circumstances, information security departments are pursuing several strategies. With greater budgetary freedom, a broad-based uptick in security spending is projected. Topping the list is increased expenditures in security tools and technologies; nearly half of the survey respondents expect an increase. A cautionary note to this type of expenditure was expressed by nearly two-thirds of the survey respondents. The incremental addition of security technologies without corresponding reduction in existing security platforms, what we term "security technology sprawl," is weighing on the security team's effectiveness and efficiency.

Increasing use of managed and professional security service providers to augment existing staff and address skill shortages is projected by nearly one-third of survey respondents. On a similar outsourcing vein, an increased use of security delivered as a cloud service is projected. Additionally, cloud adoption, in general, is expected to increase rapidly. In a bit of a dichotomy, cloud adoption relieves in-house security professionals of certain security operations that are entrusted to the cloud providers, but lingering concerns about security in cloud environments

contribute to the need for in-house security professionals to invest in cloud security education and training, and be active in managing security and compliance in cloud environments.

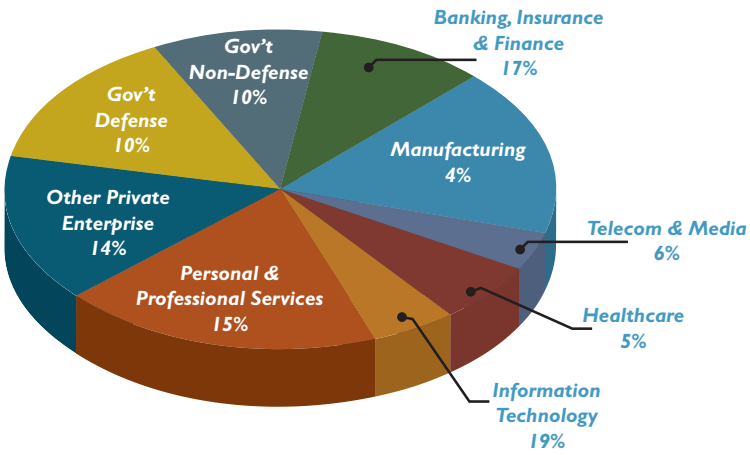
In the final assessment, the strategies of investing in security technologies, personnel, and outsourcing will be insufficient to materially reduce the workforce shortage. An expansion of security awareness and accountability throughout the organization is required. Casual attempts at security awareness and education only go so far. A more impactful approach is to embed real security accountability into other departments, in particular IT; and for the IT and security departments to function more collaboratively.

SURVEY OBJECTIVE AND METHODOLOGY

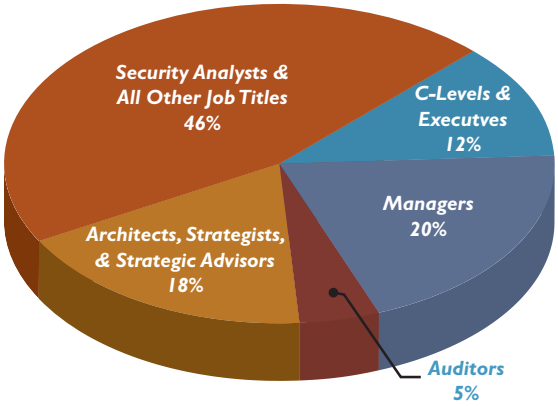
This 2015 Global Information Security Workforce Study is based on an online survey conducted over a four-month period starting in October 2014. The objective of this survey, and as presented in this study, is to gauge the opinions of information security professionals regarding trends and issues affecting their profession and careers. Designed to capture expansive viewpoints and produce statistically significant findings, the 2015 survey was completed by 13,930 qualified information security professionals; a combination of (ISC)^2 members and non-members. The diversity of survey respondents is reflected in the survey profiles in the following charts. Additionally, the distribution by organization size spanned small (1-499 employees) at 25% of the survey respondents, mid-sized (500-9,999 employees) at 32%, and large at 43%.

As (ISC)^2 has conducted similar surveys in previous years, notable comparisons to the findings of the previous surveys—the 2013 (12,396 survey respondents) and the 2011 survey (10,413 survey respondents)—are shown throughout this study. When comparisons are shown and noted, the findings are designated by study year: 2011, 2013, and 2015. When there is no designation, the findings represent the 2015 survey only.

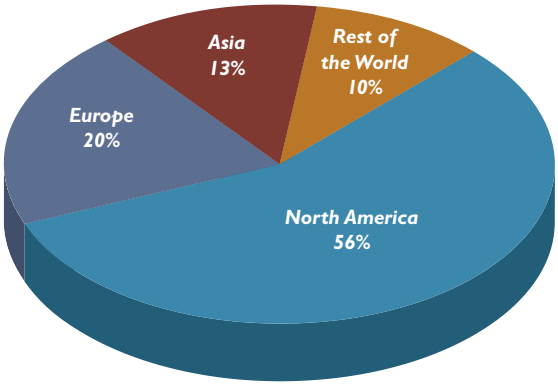
Respondents by Industry Vertical



Respondents by Job Titles



Respondents by Region



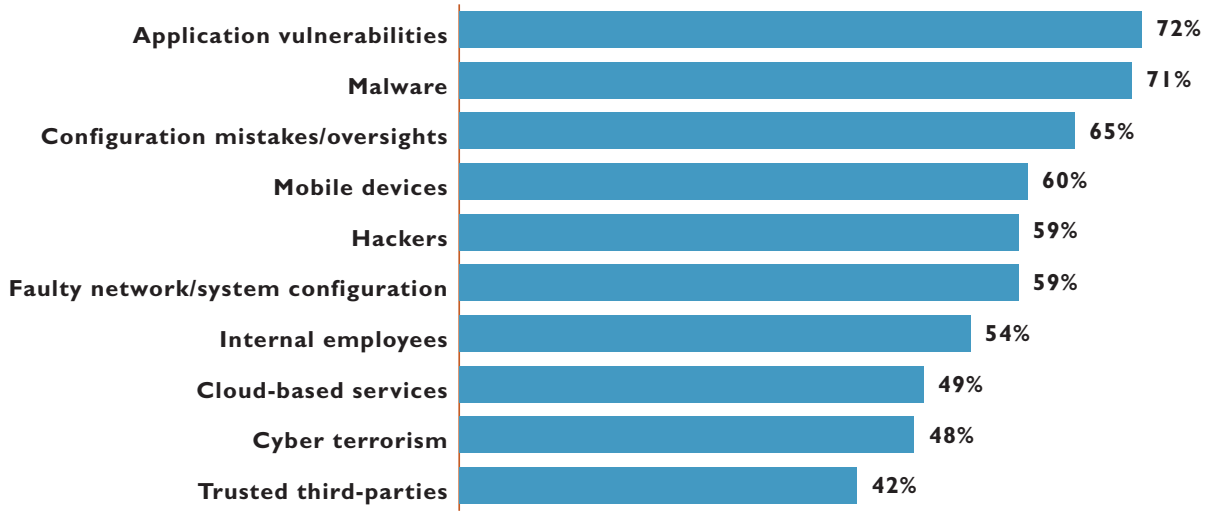
STATE OF SECURITY

The following subsections examine the state of security as seen through the eyes of the survey respondents.

Security Concerns Continue to Escalate

For information security professionals, there is no shortage of vulnerabilities to address and their adversaries are far from complacent; they constantly probe for weak links in security defenses and exploit them. Such is the case in this year's Top 10 list of security concerns. Consistent with the past two surveys, application vulnerabilities and malware top the list. These concerns are trending upward as a larger percentage of survey respondents selected this vulnerability and threat as either a top or high concern than in previous surveys. Cyber terrorism and trusted third parties also are trending upward in their levels of concern. Conversely, there is notable downward movement in the levels of concern associated with mobile devices and internal employees. Yet, as shown, each was singled out as a significant concern by a majority of the survey respondents. New to this year's survey were the selection options on configuration mistakes/oversights and faulty network/system configuration. Mirroring the weak-link of exploitive behaviors of today's cyber-attackers, both of these selection options are among the top six security concerns.

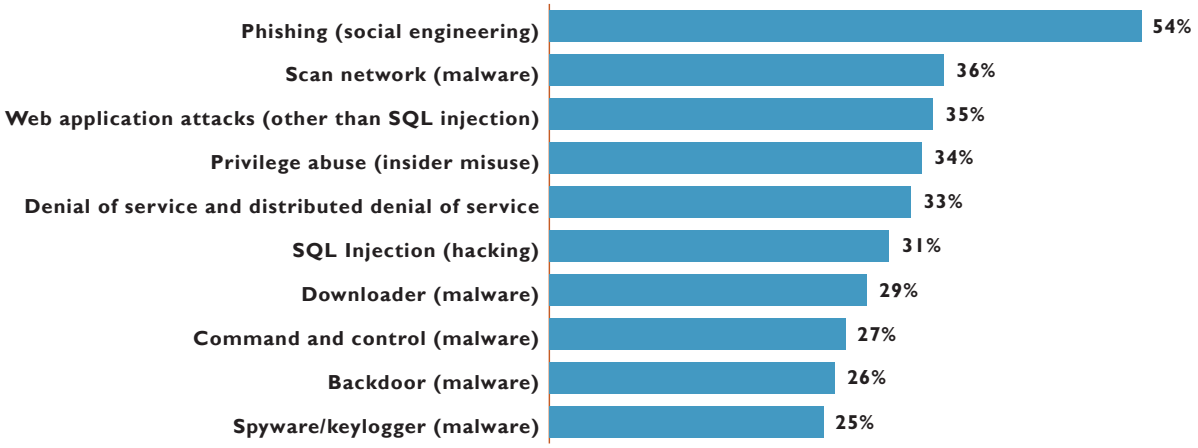
Top 10 Security Concerns (Selected as Top or High Concern)



Similar to the diversity of security concerns, the threat techniques employed by attackers and hackers are equally diverse, as shown in the next chart. Topping this list is phishing. With the evolution of attackers' capabilities, the realism and targeted approach of today's phishing campaigns rival the information security professional's efforts to elevate employees' ability to recognize, report, and leave untouched suspected phishing messages.[1] Unfortunately, just one nonchalant "click to open" or "click on this link" is sufficient to start a virulent propagation of malware across the organization's network and systems, thus highlighting the need for security awareness education and training spanning the entire organization, not just security professionals. However, regarding the high level of concern over phishing, the percent of survey respondents indicating growing demand for end-user education and training on phishing has been declining over the past three surveys (2011 - 39%, 2013 – 38%, and 2015 – 32%).

1 Also confirming the high level of concern associated with phishing is the findings included in the *Verizon 2014 Data Breach Investigation Report* (http://www.verizonenterprise.com/DBIR/2014/). Phishing has been in the top 20 varieties of threat actions in each of the past five years, rising to tenth place in 2013 and then third place in 2014.

Top 10 Common Threat Techniques (Selected as Top 2 on a 5-point, Not-Common-to-Very-Common Scale)



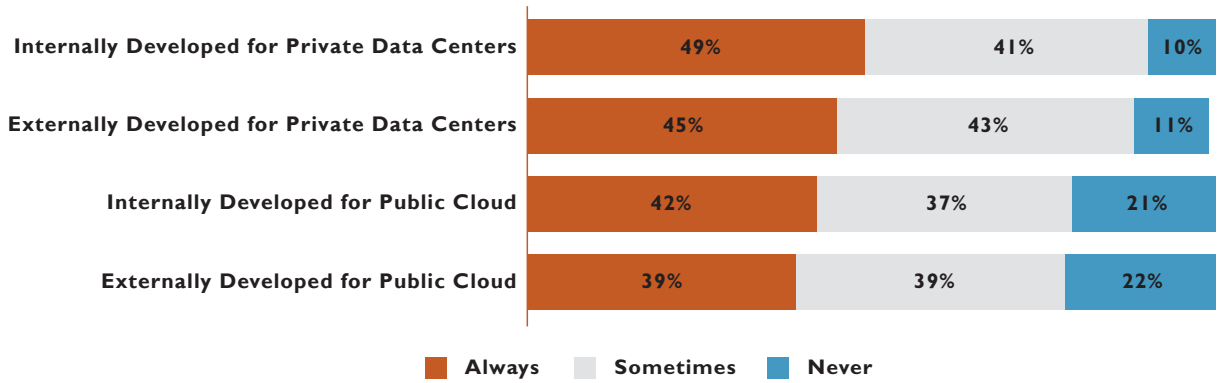
Corresponding to the high level of commonality of phishing and other techniques to distribute malware, time spent on remediation ranks high among security professionals. When asked about where they spend significant amounts of time, malware clean-up (i.e., remediating attacks and malware), as shown in the table below, was chosen by 85% of the survey respondents that function in an incident response group. Other activities that consume significant amounts of time are network monitoring and event management by security professionals in a security operations role.

Activities within *Functional Groups*	Consumes a Significant Amount of Time (2015) Percent of Survey Respondents	Compared to 2013 Survey
Incident Response		
Remediating Attacks and Malware	85%	↑
Security Operations		
Monitoring the Network	64%	Unchanged
Event Management	62%	↑

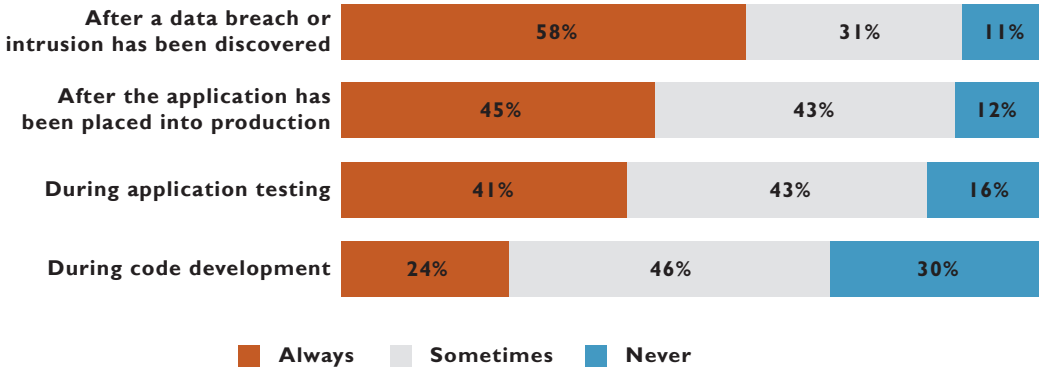
Application Vulnerability Concerns Unmatched by Remediation Efforts

With application vulnerabilities perennially being a top-rated security concern, a corresponding effort to lessen application vulnerabilities is logical. In practice, however, this is not the case. Application security scanning, a primary means to discover the existence of vulnerabilities and assess criticality, is not done at the frequency or placement (e.g., early in the software development cycle) commensurate with the security concern, as shown in the next pair of charts.

Frequency of Application Security Scanning (Percent of Survey Respondents)



When Application Security Scanning is Conducted (Percent of Survey Respondents)



Several perspectives follow from these findings that are correlated with other survey findings discussed later in this study:

- **Scanning frequency, albeit low in all cases, is more frequent for applications hosted in private data centers, where the application owner has more control over the end-to-end environment, than in public clouds** – In addition to the end-to-end control, another contributing factor to this difference could be the type of applications hosted in private data centers versus public

clouds; that is, applications processing sensitive data or essential to business-critical operations are more likely hosted in private data centers versus public clouds. As cloud adoption gallops forward (a point confirmed later in this study) and, by default, applications become more portable, the need to assess application vulnerability with equal frequency, regardless of hosting location, increases.

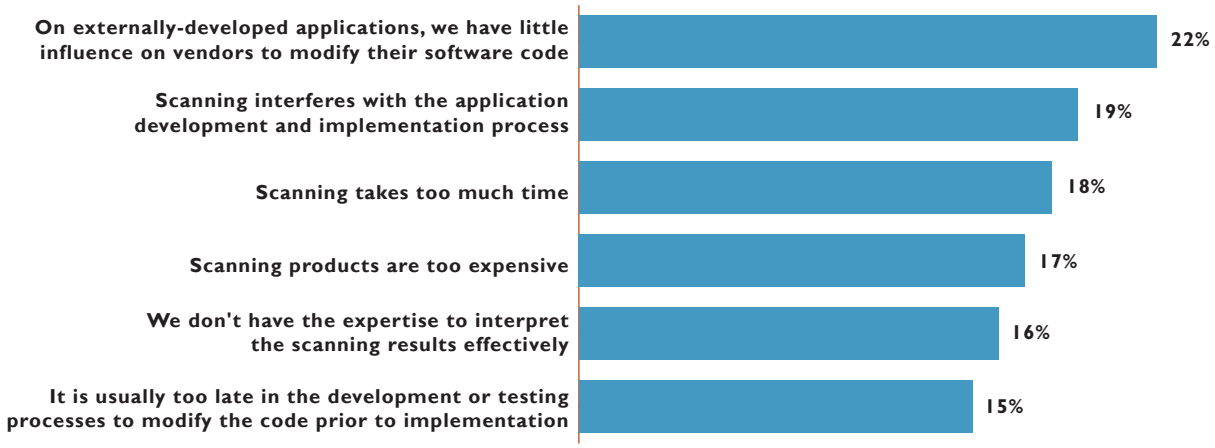
- **Isolation of workloads in public clouds is critical** – Also stemming from the frequency difference based on hosting location, applications hosted in public clouds are potentially more susceptible to exploitation of application vulnerabilities. With these survey findings as a barometer of the relatively higher vulnerability level of cloud-hosted applications, isolation of workloads among tenants in a shared cloud environment is essential in "containing" exploits that compromise one tenant so they do not contaminate other tenants in the same cloud. Discussed later in this study is the rising need for security professionals to be proficient in cloud security, both in validating the security mechanisms employed by the cloud provider and the supplemental security mechanisms that should be enacted by the cloud tenant.

- **Application scanning, like other security functions, is more reactionary than preventive** – As shown previously, the frequency of application scans is higher after an application is in production, or worse, after a breach has been discovered versus earlier in the application development cycle (i.e., code development and testing). Once in production, remediating vulnerabilities by changing the application code is unlikely, at least in the near term. Consequently, security wrappers (e.g., virtual patches) are used to lessen the potential of compromise. Although potentially effective, managing these additional layers of security adds to the security professional's responsibilities and, if left unattended, undermines the effectiveness of these additional layers. Scanning after a breach is obviously the most reactive; the vulnerability has been exploited and to a point that the organization has been harmed. It is still valuable to be done from a forensics perspective, but does little to immediately improve the organization's security posture.

- **No application is an island** – Assuming that the reported uneven scanning frequency and scanning being conducted later in the application lifecycle is partially attributable to a mix of application types (critical applications scanned earlier and more frequently than non-critical applications). Even software code used in less-critical or data-sensitive operations represents an entry point for crafty hackers. Once in, patient and experienced hackers will maximize that foothold to move laterally to reach prized assets. In other words, vulnerabilities in one application must be assessed in the broader context of connectedness (i.e., no application is an island). Correspondingly, the aforementioned significant time consumption in network monitoring and, later in this study, use of advanced analytics is prominent inmitigating app-to-app exploits.

As justifiable as application scanning is, it is no panacea. Several reasons were offered by the survey respondents as to why application scanning is not conducted. Unsuitable scanning products show up prominently in their reasons. But as will be noted later in this study, insufficient training on security technologies is a gap identified by survey respondents, too.

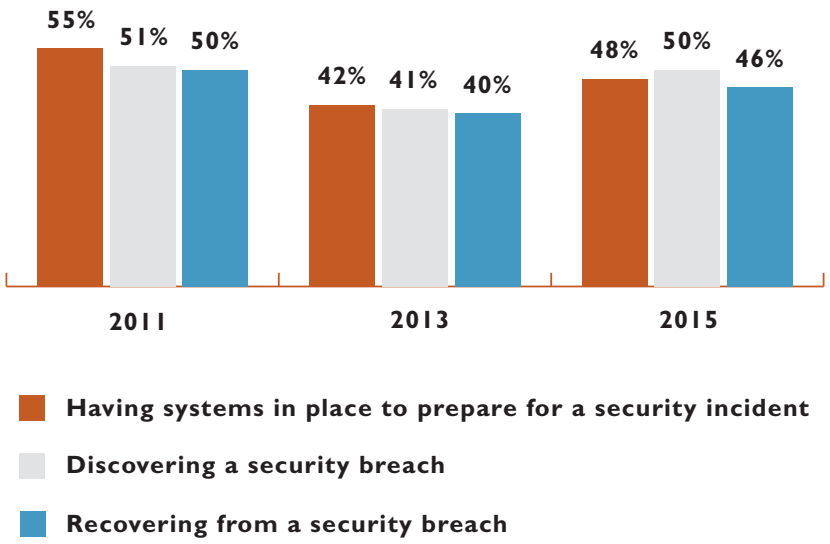
Reasons for Not Conducting Application Security Scans (Percent of Survey Respondents)



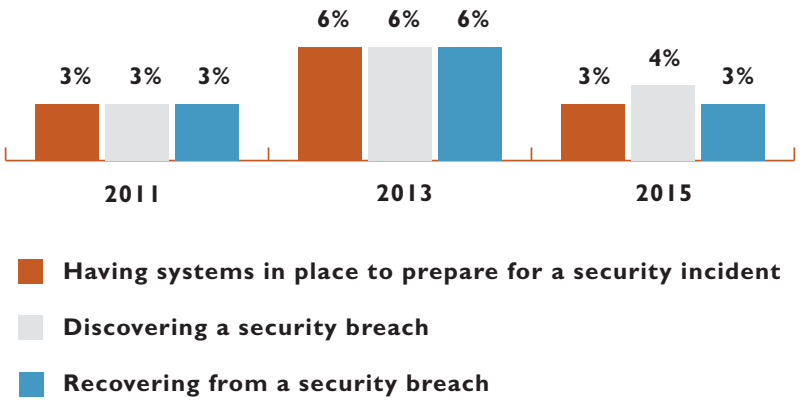
Security Readiness Stuck in Neutral

One of the illustrative questions included in the (ISC)[2] surveys over the years examines security readiness. On a backward-looking view, survey respondents are asked if their organizations improved, stayed the same, or worsened in their security readiness over the previous 12 months as measured in three areas. Those areas and the findings for each of the past three surveys are displayed in the following two charts.

Readiness Improved Over Last 12 Months (Percent of Survey Respondents)

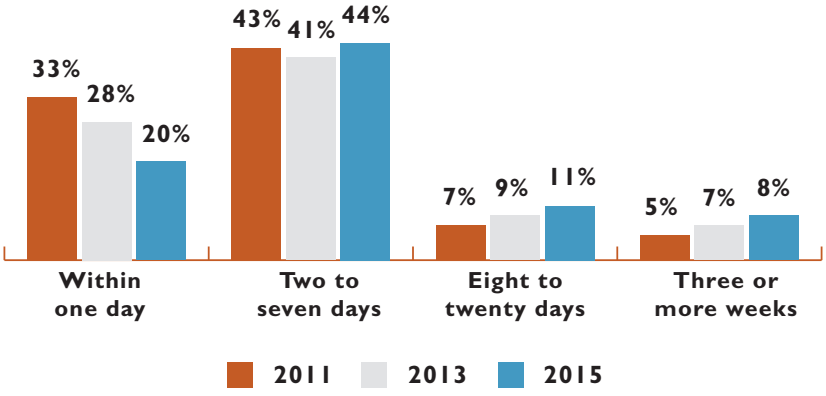


Readiness Worsened Over Last 12 Months (Percent of Survey Respondents)



Not to excessively discount the moderate improvement in readiness as reported in 2015 versus 2013, but the meaning behind these findings is that more than half of the survey respondents believe that their organizations did not improve their positions against their security adversaries. Striking a more somber note is that remediation time following a system or data compromise is lengthening, as shown in the following chart. For example, in the 2011 survey, one-third of the survey respondents indicated that remediation would occur within one day. Conversely, in the 2015 survey, that percentage dropped to one-fifth of survey respondents.

Remediation Time Following a System or Data Compromise (Percent of Survey Respondents)

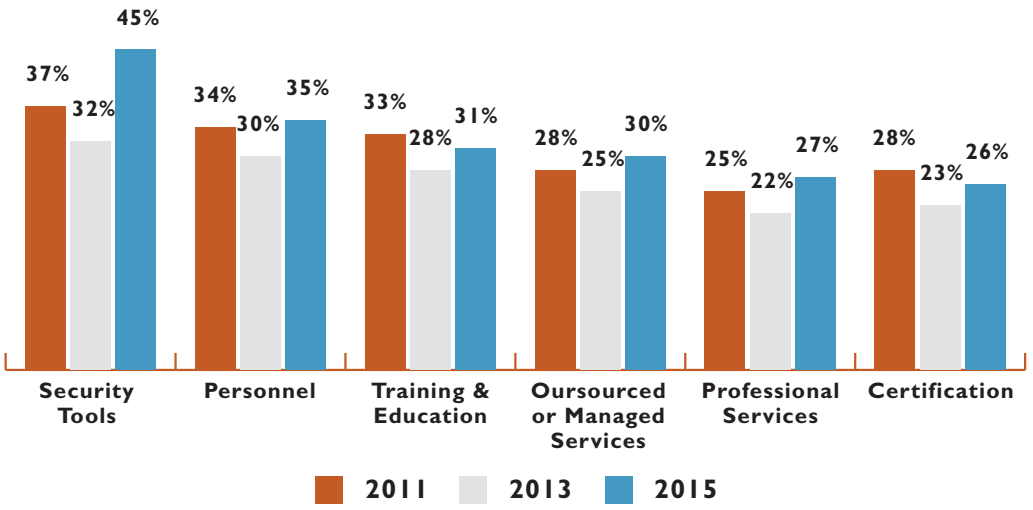


Considering the modest growth in the number of security professionals and their tenures, and Frost & Sullivan's market analysis on growth in security products and services, just staying even with the adversaries requires continuous and coordinated investments in three areas: security technologies, personnel, and external resources. Each of these areas will be examined in detail in sequential sections of this study.

INVEST TO IMPROVE

In this section, we examine the three areas in which survey respondents signaled security investments will be made over the next 12 months. The chart below captures the broad-based nature of these projected investments. Whether the investments are in security technologies (security tools including software and hardware appliances), personnel including training & education, certification, or external resources (use of outsourced or managed security services and professional security services), all categories are showing more respondents projecting increased spending than in 2013. The security tools category has the largest survey-over-survey percentage point gain. Additionally, overall and consistent across surveys, C-levels—individuals with the greatest control over security spending—were more bullish on spending with a greater percent of projected spending increases than managers. On projected declines, the percent of respondents projecting declines in spending over the next 12 months was in the single digits in 2015; and 2015 percentages are lower than the percentages for 2013 and 2011 in all categories.

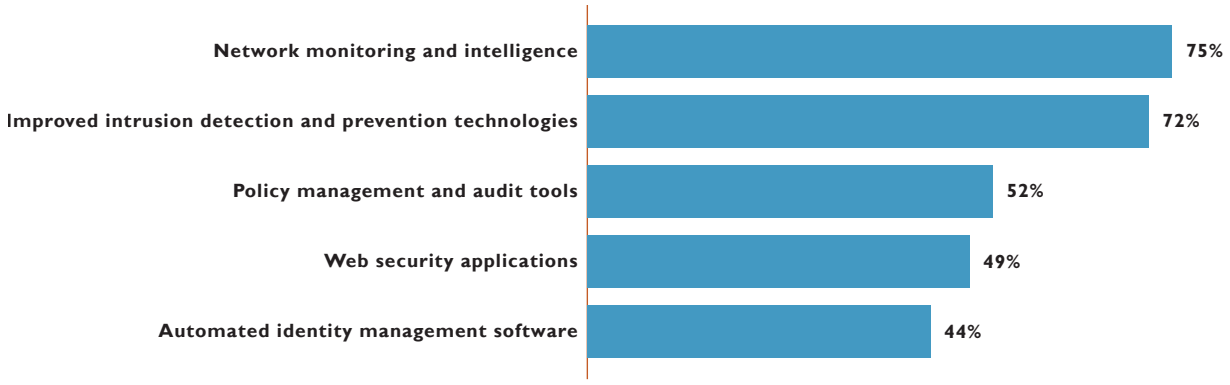
Where Increases in Information Security Spending are Projected (Percent of Survey Respondents)



Invest to Improve: Security Technologies

As previously shown, the percentage of survey respondents predicting spending increases in security technologies is the highest across categories and previous surveys. Where will that security technology spending be directed? According to the survey respondents, security tools that improve their ability to detect abnormal or threatening behaviors lead the list versus more static defenses, such as firewalls and network segmentation. This datum is consistent with the prevailing sentiment that network and system compromises will occur even with the best defensive strategy. The fluidity of the environments that require protection and advancing adversaries are among the factors that support this sentiment. Accepting the likelihood of compromise, there is a correspondingly high level of emphasis expressed by the survey respondents on improving the means to rapidly and reliably detect compromises.

Top 5 Technologies that Significantly Improve Security (Percent of Survey Respondents)

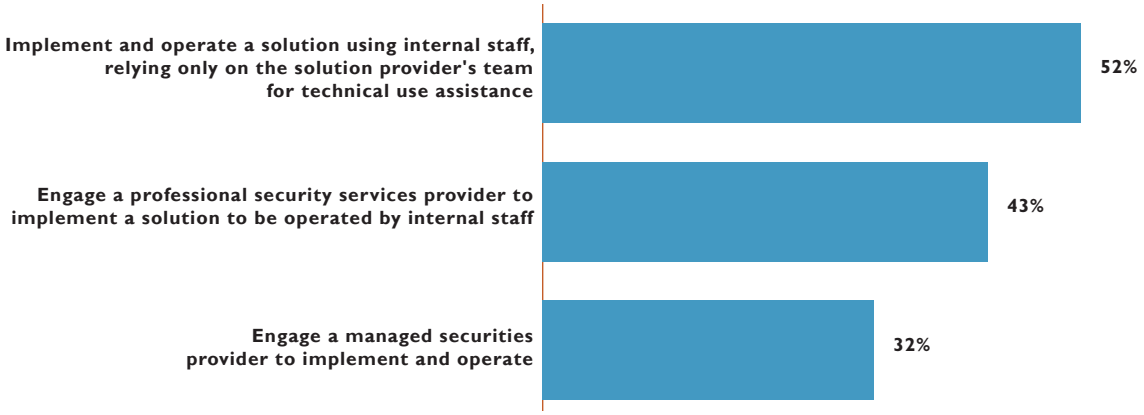


Delving deeper into the rising detection requirement, the 2015 survey included questions on the adoption of advanced analytics in the detection of advanced forms of malware. According to the survey results, momentum is building for the adoption and use of advanced analytics. More than one-third of the survey respondents indicated that advanced analytics are already implemented or in the process of being implemented. As customary with newer forms of security technologies, larger organizations are faster adopters than small businesses. This same dynamic is true with advanced analytics: 42% of respondents in large organizations (more than 10,000 employees) indicated that advanced analytics are implemented or in the process of being implemented compared to 26% of respondents in small businesses (less than 500 employees).

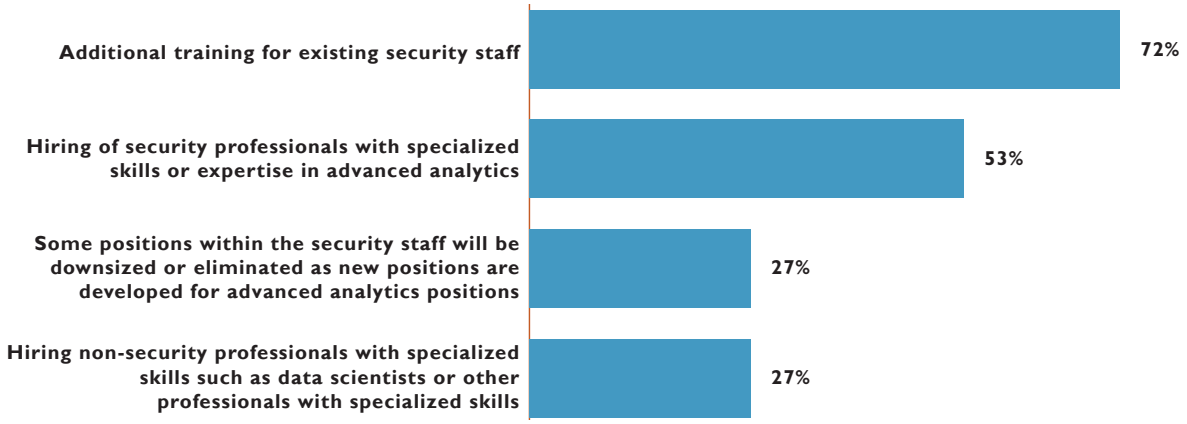
Use of Advanced Analytics for Detection of Advanced Malware (Percent of Survey Respondents)

In the use of advanced analytics, slightly more than half of the survey respondents indicated that an internal-only, do-it-yourself (DIY) approach will suffice. Use of outside assistance, either exclusively or as a complement to internal staffing, was also prominently indicated. Regardless of DIY or outside assistance, the survey respondents were together on the need for specialized training and skills to optimize the benefits of advanced analytics solutions.

Approaches to Implementing and Operating Advanced Analytics (Likely or Very Likely)



Staffing and Training for Advanced Analytics (Very Likely or Somewhat Likely)



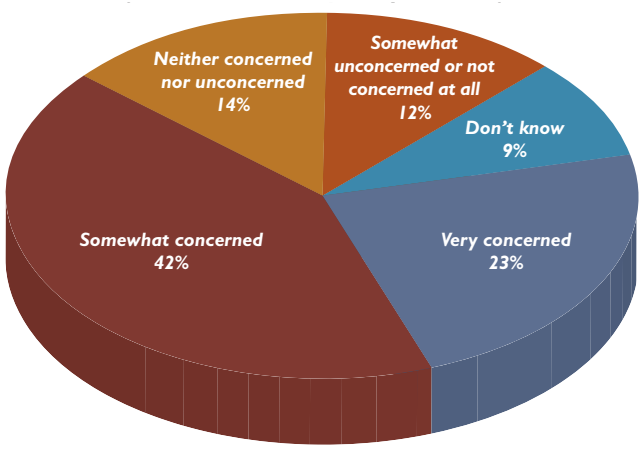
Sprawl in Security Technologies is a Material Concern

Also new in the 2015 survey were questions regarding security professionals' views on security technology sprawl—concern, causes, and impact. This is a particularly relevant question in light of the aforementioned projected spending increases in security technologies with the stagnant improvement in security readiness. For topic clarity, the following statement preceded the sprawl-related questions in the survey:

> "Today, the information security industry is seeing a greater number of security technology products and an increasing number of security vendors and management consoles. This is sometimes referred to as ineffective architecture, or sprawl."

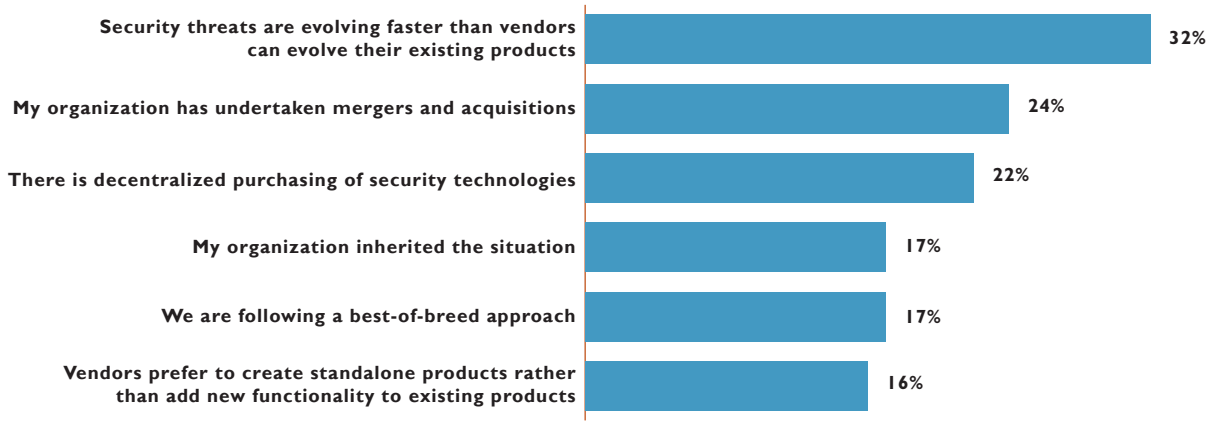
The survey respondents were fairly uniform in their concern about security technology sprawl. Approximately two-thirds listed their concern as either somewhat or very concerned. This voiced concern was not exclusive to managers; respondents across all job titles expressed nearly identical levels of concern.

Security Technology Sprawl Concern (Percent of Survey Respondents)



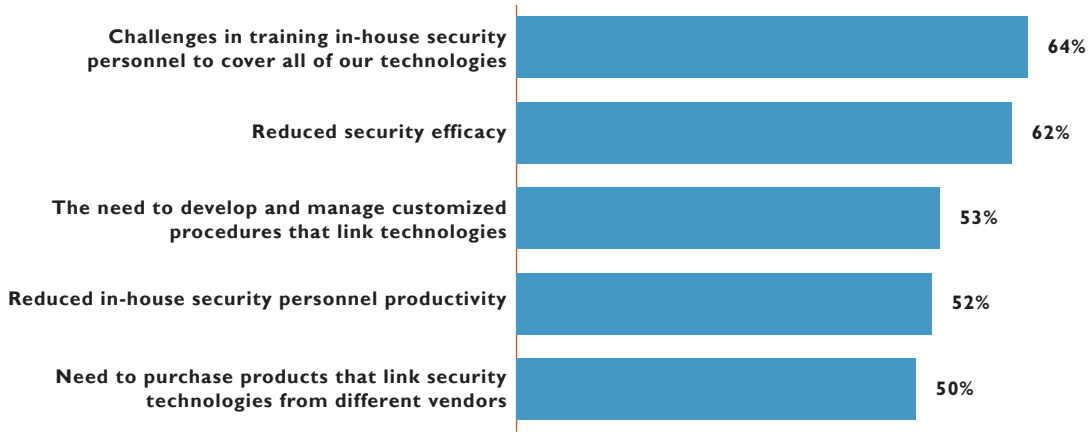
When prompted for reasons contributing to security technology sprawl, there was a wide distribution of cited reasons.

Top Reasons for Security Technology Sprawl (Percent of Survey Respondents)



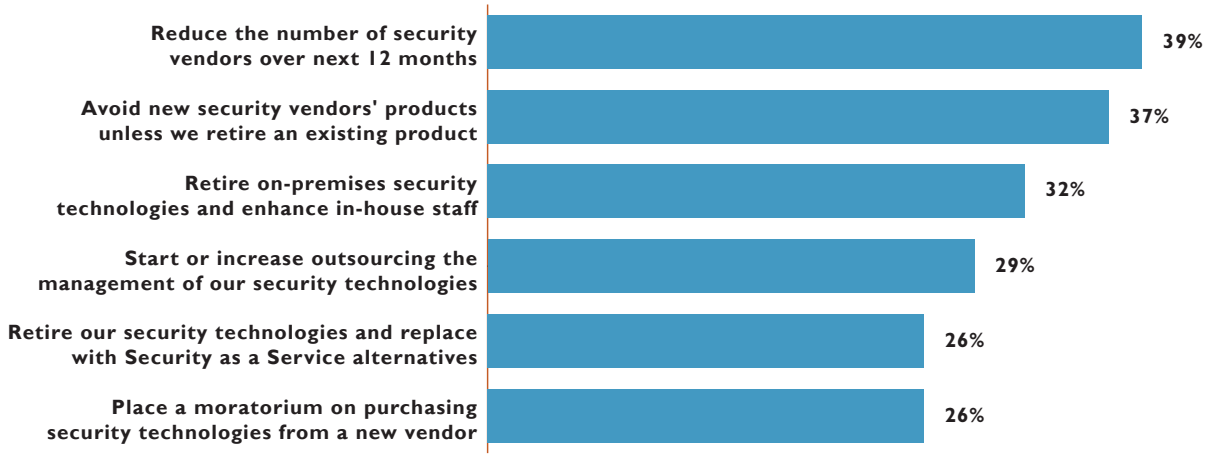
Several implications of security technology sprawl were cited by 50% or more of the survey respondents. Collectively, the implications fall into two categories: reduced security efficacy and productivity, and increased need for training and workarounds.

Top 5 Implications of Security Technology Sprawl (Percent of Survey Respondents Selecting Top or High)



With security technology sprawl, a situation that builds over time, reversal will also take time. Similarly, a single strategy is unlikely, as confirmed by survey respondents.

Strategies To Combat Security Technology Sprawl (Percent of Survey Respondents Selecting Very or Somewhat Likely)



Invest to Improve: Personnel

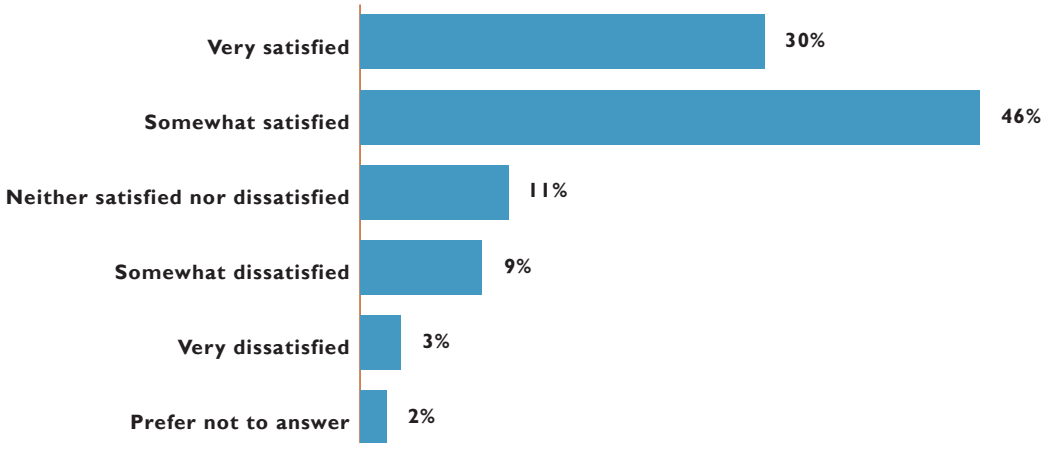
Personnel is the second of three areas in which organizations make investments in order to improve their cyber defensive posture. Investing in personnel is more complex than the other areas, as we will see. Personnel investment requires a number of monetary and non-monetary initiatives for maximum return.

The issue of scarcity is important to be introduced as a prelude to this section as security professional scarcity is a consistent theme voiced by the nearly 14,000 security professionals that responded to the 2015 survey. Despite satisfaction with their jobs, current data and historical perspective on employment, salaries, and tenure point to difficulty in attracting sufficient numbers of qualified entrants into the profession.

State of the Information Security Profession

Given the environment in which security professionals work, a certain amount of discontentment with their current roles would be understandable, if not expected. However, such an assertion is simply not correct. Better than three out of every four security professionals characterized themselves as either "Somewhat satisfied" or "Very satisfied," with 30% of the total sample characterizing themselves as "Very satisfied."

Overall, How Satisfied are You in Your Current Position? (Percent of Survey Respondents)

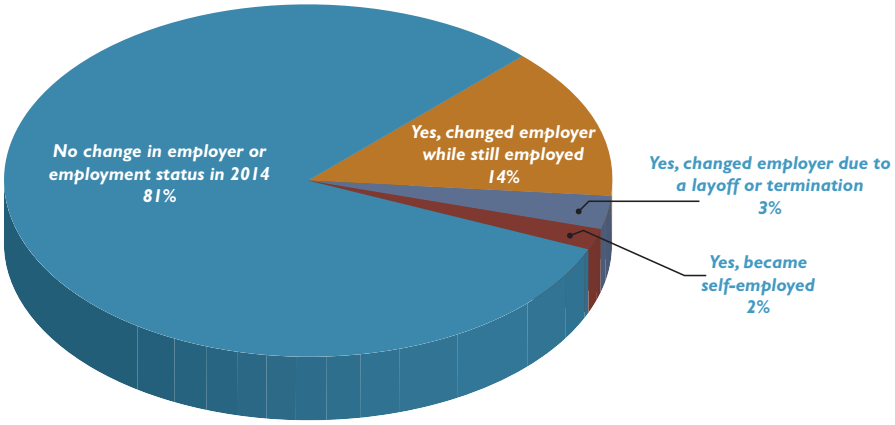


Rising Retention Difficulties

High job satisfaction facilitates employee retention. Many other factors are clearly relevant; employee churn is an issue for employers of security professionals in spite of security professionals' satisfaction with their current positions.

In a single year, 2014, nearly one in five security professionals changed employers or employment status. Across the 2011, 2013, and 2015 surveys, churn of nearly 20% is the highest that has been seen.

Did You Change Your Employer or Employment Status in 2014? (Percent of Survey Respondents)



Correspondingly, having 14% of respondents reporting that they "changed employers while still employed" was also the highest percentage across the three surveys. Rising churn is the first sign of rising security professional scarcity.

Dramatic Rise in Salaries

Salaries reached their highest level as reported in the 2015 survey for both (ISC)^2 members and non-member security practitioners. Collectively, the average annual salary among the security professionals surveyed was US$97,778. Differences between (ISC)^2 members and other security practitioners exist. Non-member security practitioners reported an average annual salary of US$76,363. The salaries among security professionals with an (ISC)^2 membership averaged US$103,117 annually, a 35% premium over non-members.

Worldwide	(ISC)^2 Members			Non-Members		
	2011	2013	2015	2011	2013	2015
Average Annual Salary	$98,605	$101,015	$103,117	$78,494	$75,682	$76,363
Survey-over-Survey		2.4%	2.1%		-3.6%	0.9%
Membership Premium	26%	33%	35%			

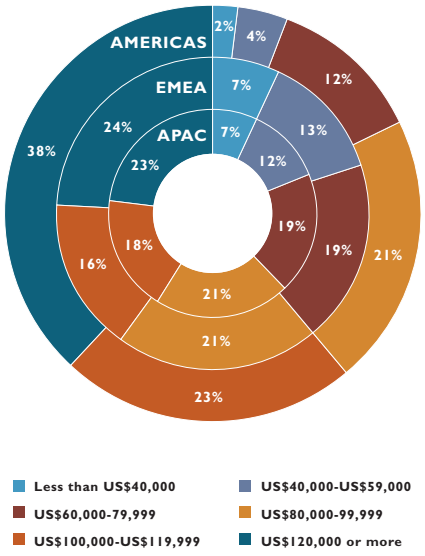
More impressive than net salaries reported, security professionals salaries showed impressive gains since the 2013 survey. The average salary increased 2.1% for members and 0.9% for non-members.

To further confirm relative salary levels, change, and membership premium, we examined salaries for a large subset of the survey respondents: security analysts employed in the US private sector. The survey findings further confirm—after normalizing for job title, country location, and employer sector—that salaries are rising and the membership premium is robust over the four-year period.

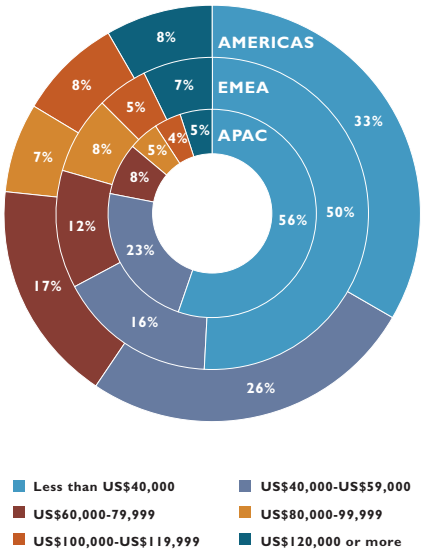
US-Based Security Analysts in Private Sector	(ISC)^2 Members with CISSP Certification			Non-Members without CISSP Certification		
	2011	2013	2015	2011	2013	2015
Average Annual Salary	$93,027	$94,316	$99,759	$76,402	$76,957	$81,301
Survey-over-Survey		1.4%	5.8%		0.7%	5.6%
Membership Premium	22%	23%	23%			

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 survey respondents in developed countries and second in developing countries.

DEVELOPED COUNTRIES-2015

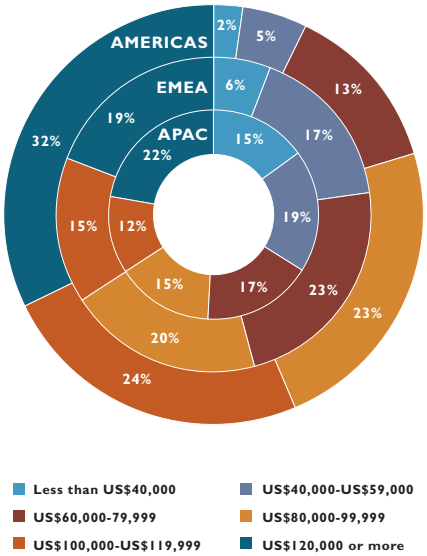


DEVELOPING COUNTRIES-2015

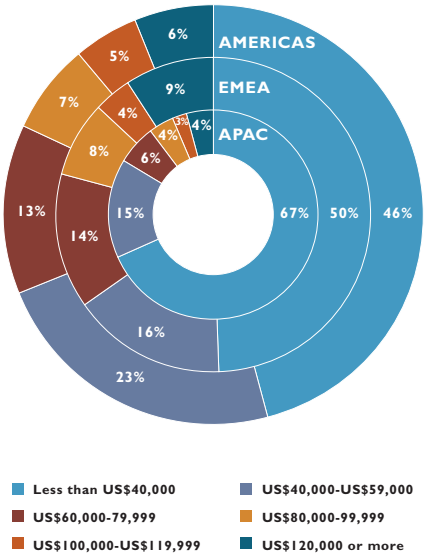


Security profession scarcity is reaching beyond developed countries, increasing salaries in developing countries as well. In comparing the 2015 survey with the 2013 survey, a significant change occurred in the distribution of salaries in developing countries in the Americas and APAC regions. In 2015, salaries of less than US$40,000 comprised 33% of the Americas survey respondents in developing countries, 13 percentage points lower than in the 2013 survey. APAC had 56% of salaries of less than $40,000 in 2015, 11 percentage points lower than the 67% in the 2013 survey.

DEVELOPED COUNTRIES-2013



DEVELOPING COUNTRIES-2013



Where is the Influx of New Talent?

Despite the increase in salaries, the average tenure among security professionals is stabilizing. Although stabilizing for members and non-members, the difference in average tenures between (ISC)² members and non-members is notable as a partial attribute for the higher salaries reported by (ISC)² members.

Worldwide	(ISC)² Members			Non-Members		
	2011	2013	2015	2011	2013	2015
3 years or less	3%	2%	2%	15%	11%	15%
4 - 6 years	16%	10%	10%	26%	19%	18%
7 - 10 years	38%	26%	26%	28%	24%	24%
11 - 15 years	26%	32%	32%	17%	22%	20%
16 - 25 years	13%	20%	20%	9%	15%	15%
More than 25 years	5%	9%	9%	4%	9%	7%
Average Tenure (Years)	11.4	13.4	13.4	9.3	11.4	11.0

Among US-based security analyst respondents in the private sector, a similar pattern is seen. US (ISC)² members with the CISSP certification have seen the average tenure grow from 10.5 years in 2011 to 12.7 years in 2015. Non-member US respondents had tenures that grew from 6.4 years to 8.9 years.

US-Based Security Analysts in Private Sector	(ISC)² Members with the CISSP Certification			Non-Members w/o CISSP Certification		
	2011	2013	2015	2011	2013	2015
Average Tenure (Years)	10.5	12.0	12.7	6.4	8.9	8.9

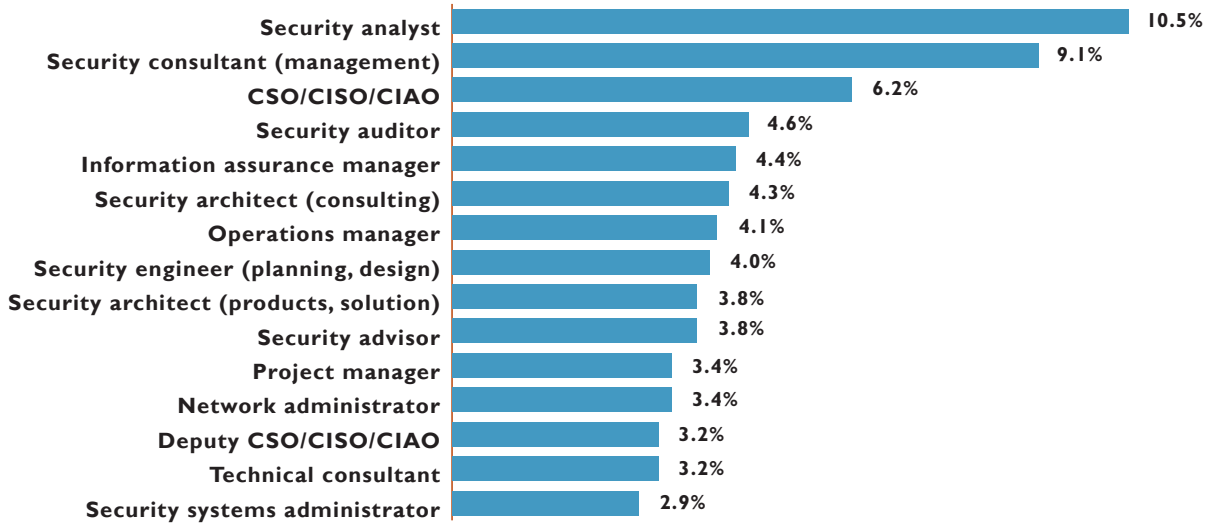
What is being seen in the employment of security professionals can be explained by basic economics. The demand for security professionals is growing, but the supply of security professionals is not growing at the same rate. The result is growing salaries.

Skills and Job Roles Needed

Security analyst and security consultant (management) dominate job titles of the respondents in the 2015 study. Security analysts are on the front lines of cybersecurity efforts to keep attackers at bay. Security consultants reflect the importance of outsourcing in information security. The importance of outsourcing will be elaborated upon later in this study. Information assurance manager was a new selection in the 2015 survey and makes its debut at the number five slot, providing confirmation of the increasing importance of that function.

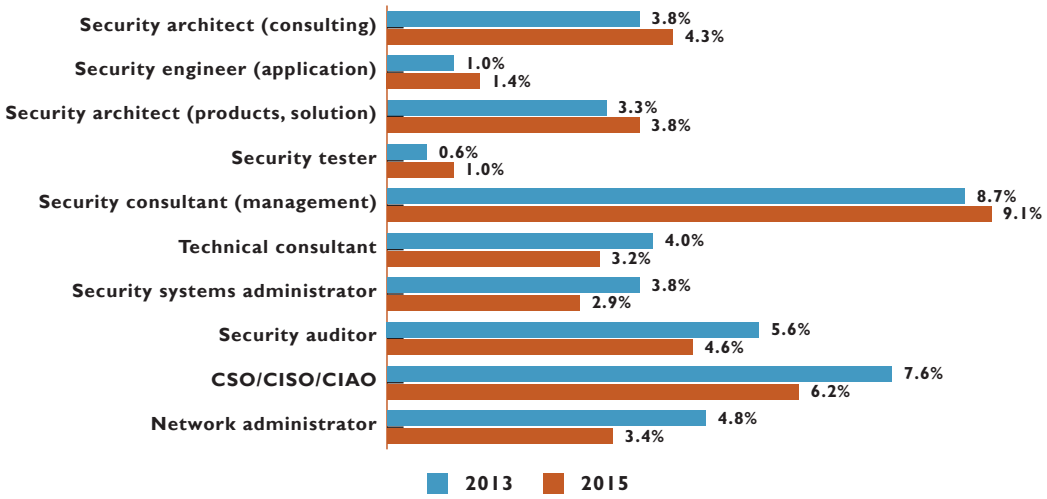
Which one of the following job titles or categories best describes your current position?

(Percent of Survey Respondents)



Examining changes in job titles from the 2013 survey to the 2015 survey, demand for security architects (consulting) leads job growth (3.8% of survey respondents in 2013 versus 4.3% in 2015). Security engineers (application) and security architect (products, solution) are the next two in the top five leaders in job title growth. Security consultant (management), security tester, and security engineer round out the top five.

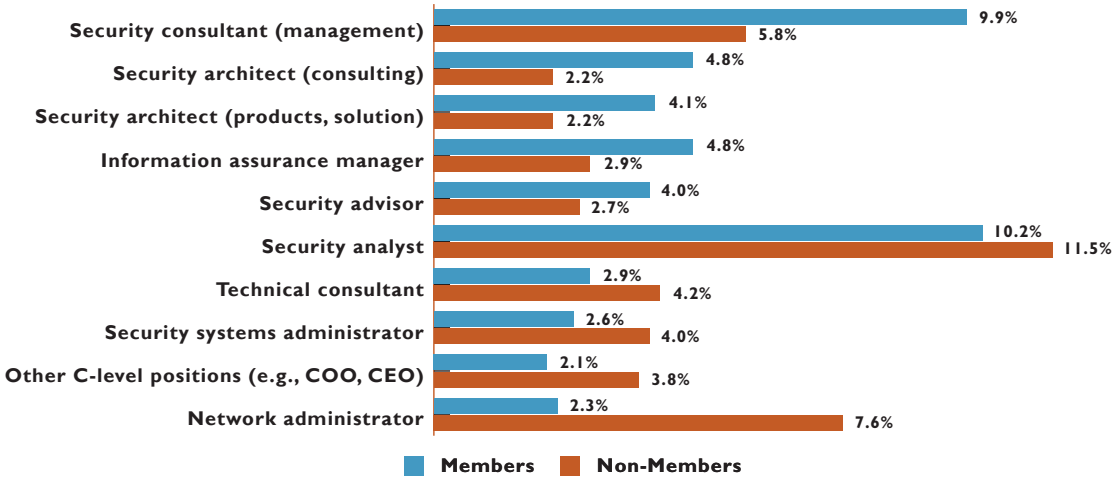
Job Titles: 2013 versus 2015 (Percent of Survey Respondents)



The top five declining job titles suggest a change in the relationship between IT and security professionals. Network administrator, CSO/CISO/CIAO, security auditor, security systems administrator, and technical consultant lead the job title declines. The functions that were accomplished by these job titles are most certainly being done, but those tasks are now likely being increasingly accomplished by IT personnel who do not necessarily view themselves as pure security professionals. The survey findings suggest that security tasks are increasingly being implemented by IT functions as directed by professionals with higher levels of security expertise, creating a security force multiplier effect.

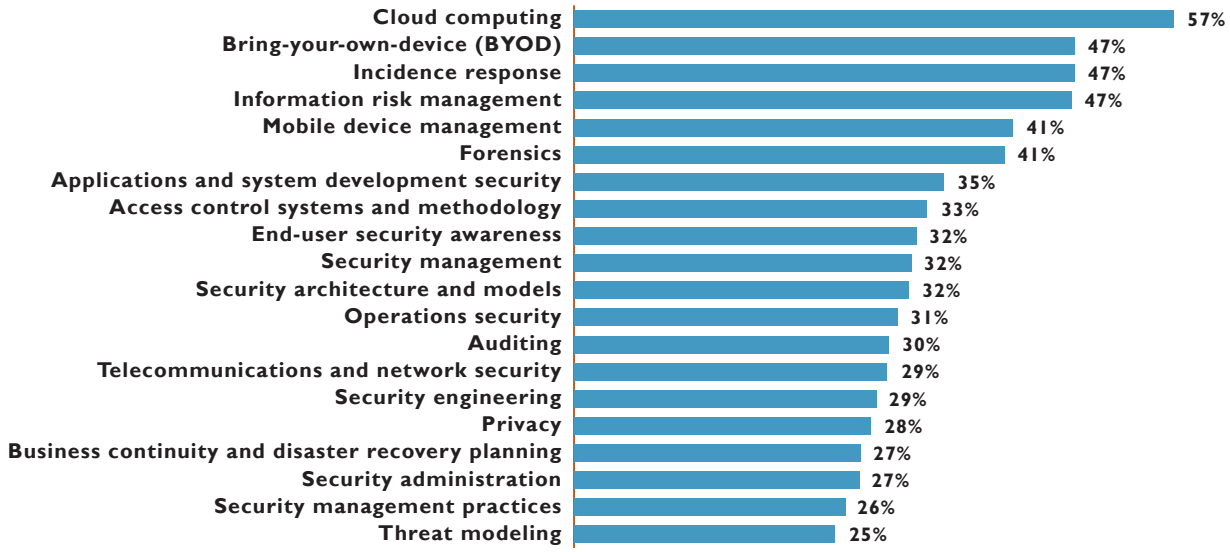
Viewing the difference in titles between (ISC)^2 members and non-members provides further confirmation of the IT force multiplier effect. (ISC)^2 members tend to be more specialized, having job titles that suggest performing more specialized security functions. (ISC)^2 members more commonly have job titles of security consultant and security architect than non-members. Non-members are much more likely to have the title of network administrator, suggesting an IT generalist role that has significant security responsibilities.

Job Titles: Members versus Non-Members (Percent of Survey Respondents)



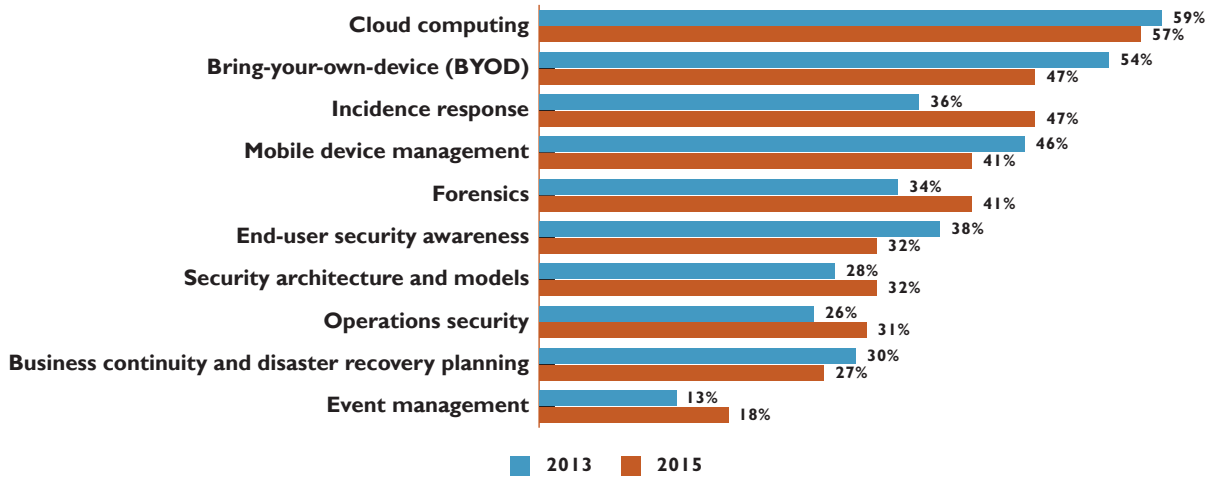
The top area for training and development for security professionals over the next three years is dominated by the technologies that require protection. Not surprisingly, cloud computing and bring-your-own-device (BYOD) top the list. Other technology-related topics include information risk management, applications and systems development, and access control.

In which areas of information security do you see growing demand for training and education within the next three years? (Percent of Survey Respondents)



Survey-over-survey analysis reveals some significant changes in the areas in which security professionals are directing their training and education focus. Although significant on an absolute basis in the 2015 survey, BYOD and cloud computing have reduced importance to security professionals. Likely a reflection of the changing threat landscape, a greater emphasis is being placed on remediating breaches. Topics such as incident response, forensics, and event management are resonating strongly.

In which areas of information security do you see growing demand for training and education within the next three years? 2013 versus 2015 (Percent of Survey Respondents)

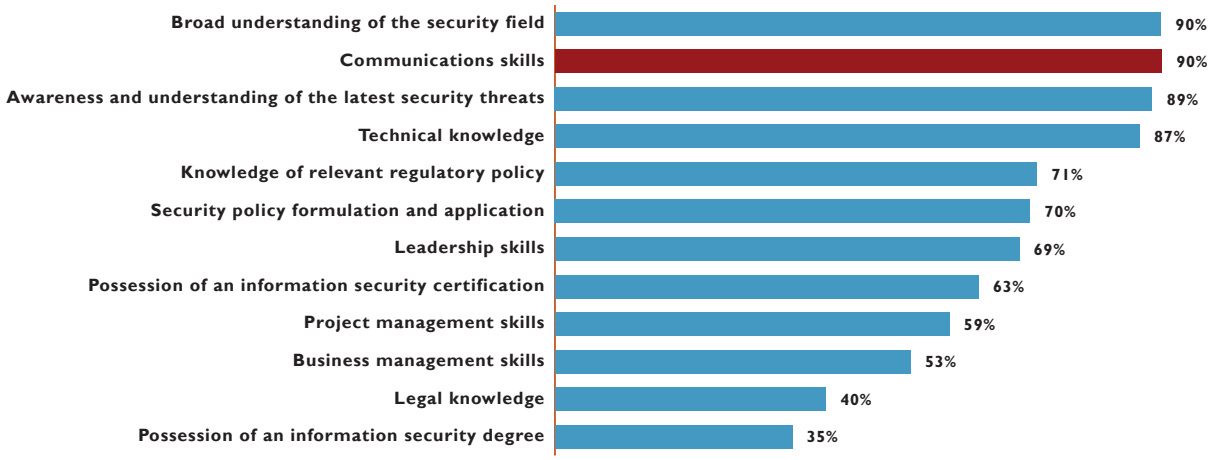


Are Security Professionals Focusing on the Right Training Requirement?

The security profession is a highly specialized and knowledge-intensive profession. The training needs expressed by the survey respondents are justified. However, the study respondents may have expressed needs for additional training that they do not recognize.

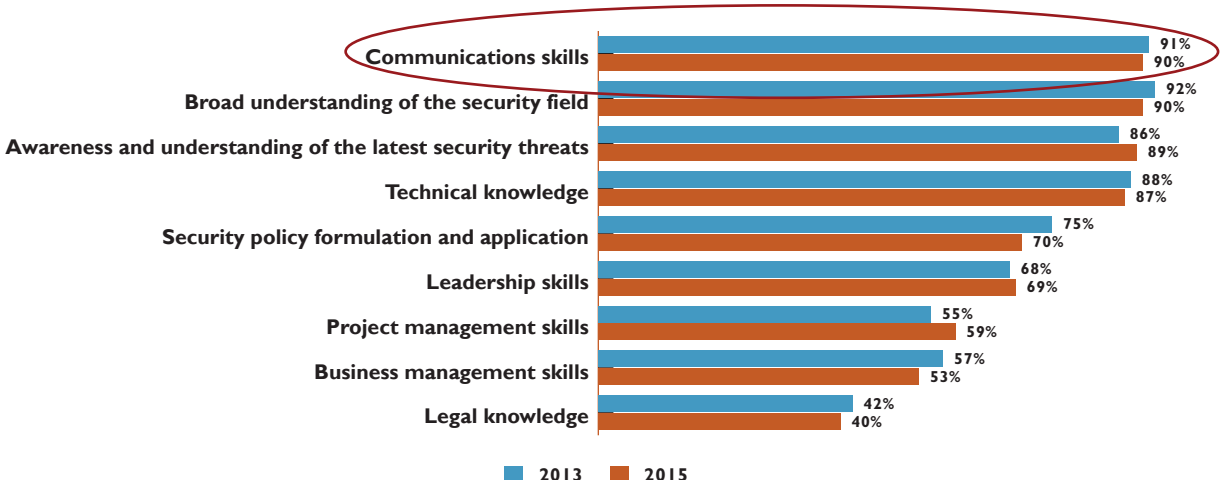
When asked about the attributes that make one successful in information security, broad understanding of the security field was the top response (based on top two box selections). Communications skills was second, ahead of selections such as technical knowledge and awareness, and understanding of the latest security threats.

How would you rate the importance of each of the following in contributing to being a successful information security professional? (Percent of Survey Respondents Selecting Top two points on a five-point Importance Scale)



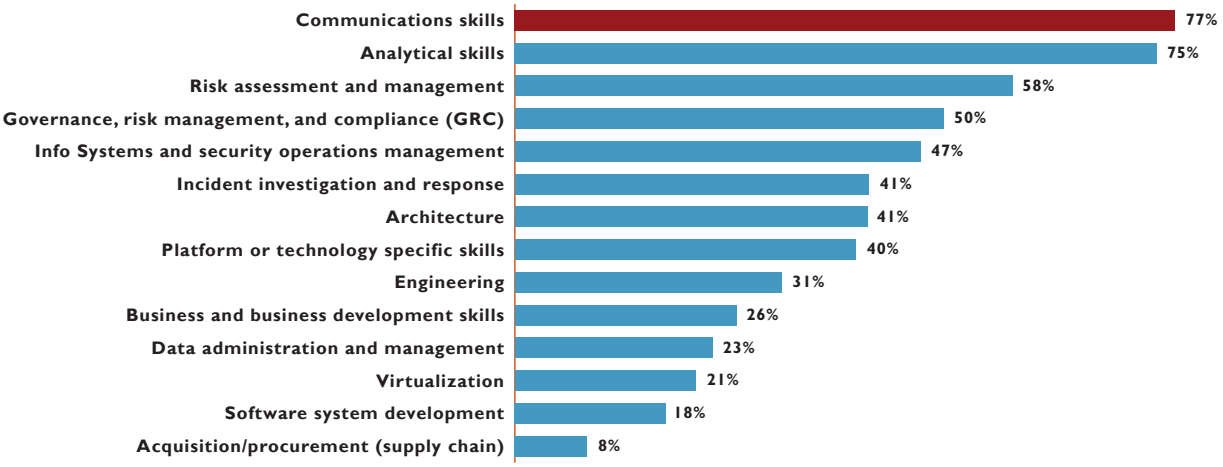
The importance of communications skills is not new. In comparing 2015 study results to 2013 study results, a negligible difference exists between the 2013 and 2015 surveys on the importance of communications skills in being a successful information security practitioner.

How would you rate the importance of each of the following in contributing to being a successful information security professional? (Percent of Survey Respondents Selecting Top two points on a five-point Importance Scale)



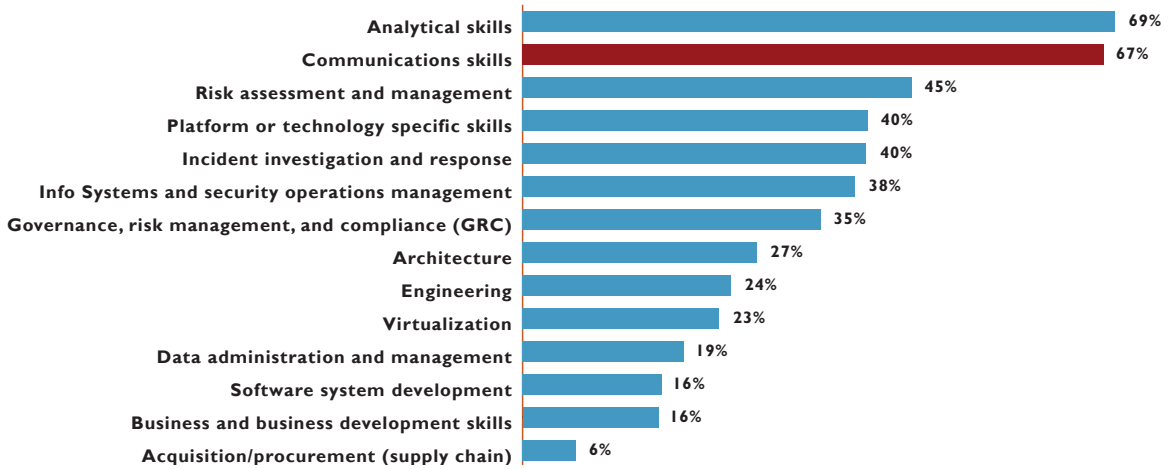
When reporting how important various skills and competencies are to career success, communications skills rank as the single-most important attribute. Interestingly, analytical skills, another soft skill, ranked second, ahead of more concrete competencies such as architecture; incident investigation and response; info systems and security operations management; and governance, risk management, and compliance.

How significant were each of the following skills and competencies in information security in achieving your current position or level? (Percent of Survey Respondents Selecting Very Significant)



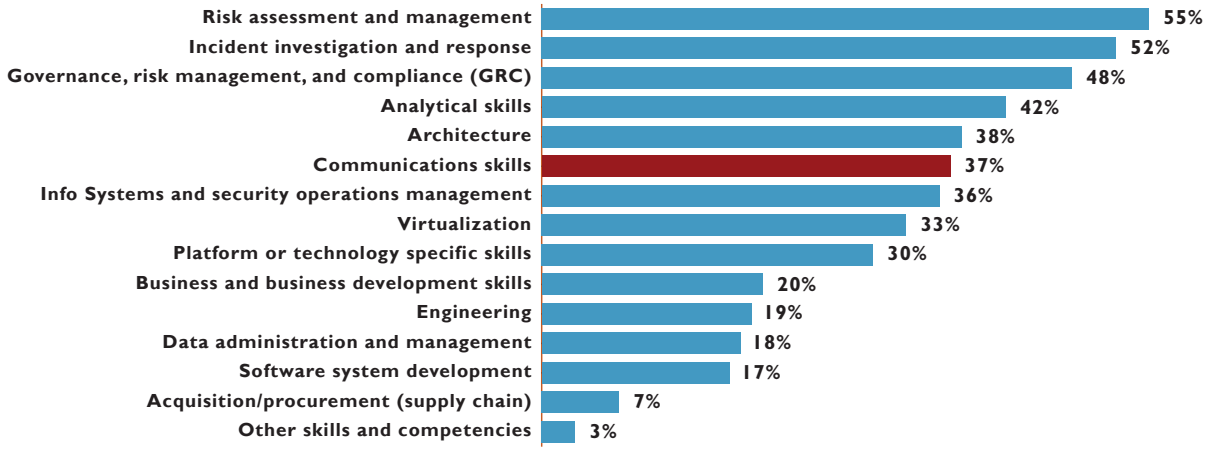
Those who recruit entry to mid-level security professionals place heavy emphasis on communications skills. In fact, significantly more respondents ranked communications skills as "very important" in hiring decisions than risk assessment and management, the third-highest ranked factor.

How important are each of the following skills and competencies when recruiting new entry to mid-level information security professionals to your organization? (Percent of Survey Respondents Selecting Very Important)



However, when considering training priorities over the next three years, communications skills failed to carry a similar level of significance. Communications skills ranked sixth on the list behind other skills and competencies. This disparity begs the question as to whether security professionals should increase their emphasis on communications skills or on technical skills.

What are the skills and competencies that you will need to acquire or strengthen to be in a position to respond to the threat landscape over the next three years? (Percent of Survey Respondents)



Corresponding to the rising importance of communications and problem-solving skills, higher levels of education, where these skills are put to a greater test, are populating the profession. Correspondingly, salaries are rising.

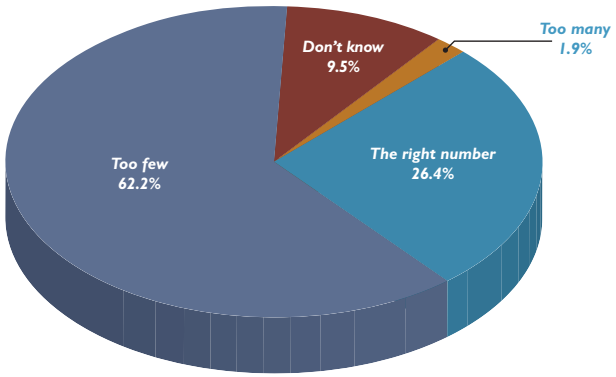
Highest Level of Education Completed	Percent of (ISC)² Members (Current)	Trend
High school (or equivalent upper secondary)	10%	↓
Bachelors (or equivalent post-secondary)	44%	↓
Master's (or equivalent first stage of tertiary education)	43%	↑
Doctorate (or equivalent second stage of tertiary education)	3%	Unchanged

Annual Salary Range	Percent of (ISC)² Members (Current)	Trend
$120,000 or more	32%	↑
$100,000 to $119,999	20%	Unchanged
$80,000 to $99,999	19%	↓
$60,000 to $79,999	13%	↓

Hiring Challenges

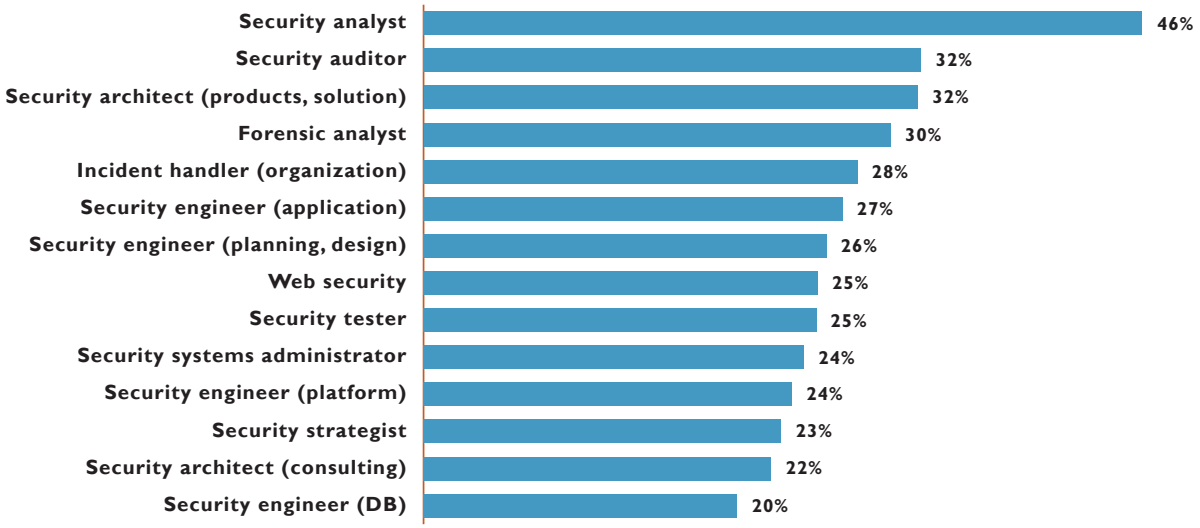
The clear message from security professionals is that companies are challenged to appropriately staff the security function. Almost two of every three respondents from the study felt there were too few information security workers. In contrast, a low 1-in-50 felt that there were too many.

Would you say your organization currently has the right number of information security workers, too few, or too many?



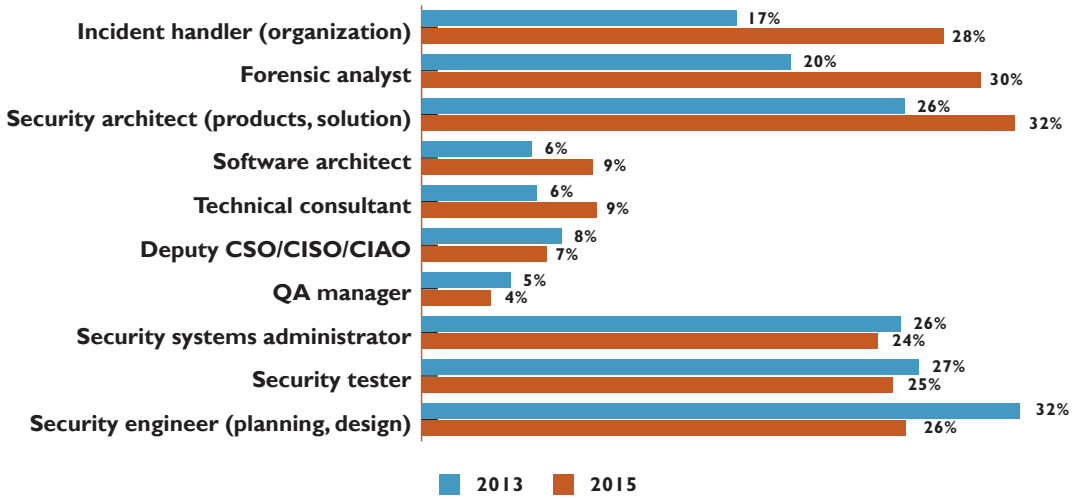
Security analyst tops the list of positions that are in most demand, with 46% reporting a staffing deficiency at that position in their organization, 14 percentage points higher than the second most-needed position: security auditor. Security architect (products, solution), forensic analyst, and incident handler (organization) round out the top five positions needed.

Of which of the following job titles or categories are there currently not enough of within your organization?
(Percent of Survey Respondents)



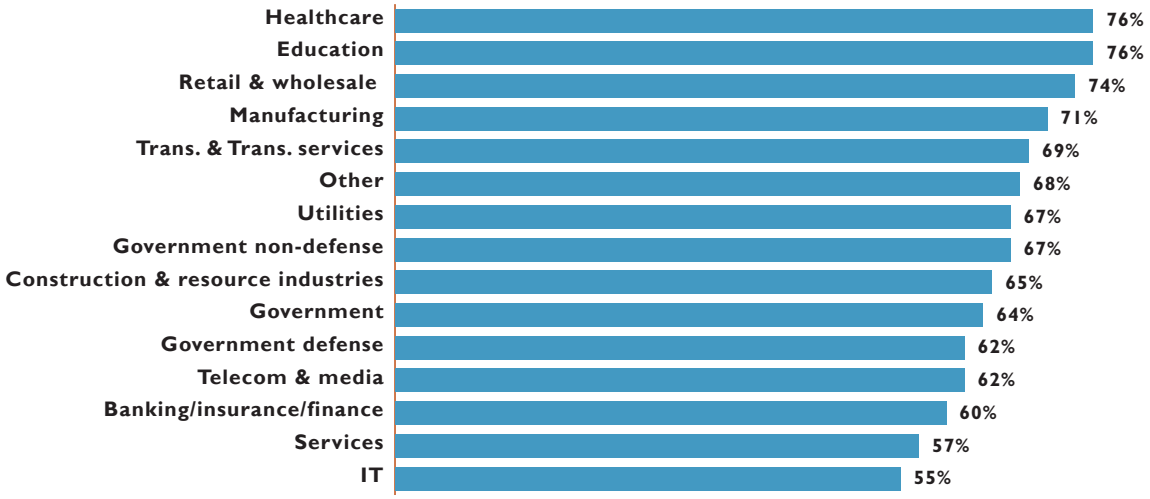
After examining the survey-over-survey changes in job titles needed, congruence is seen between changes in the job titles needed and the areas in which security professionals are placing their training and education focus. The positions that saw the largest survey-over-survey change was incident handler and forensic analyst. Remember, the top areas seeing an increase in training and education focus were incidence response and forensics. The top declines were seen in job titles that might be accomplished by individuals currently in IT roles.

Of which of the following job titles or categories are there currently not enough of within your organization? Select as many as apply. Top 5 Positive and Negative Survey over Survey Differences



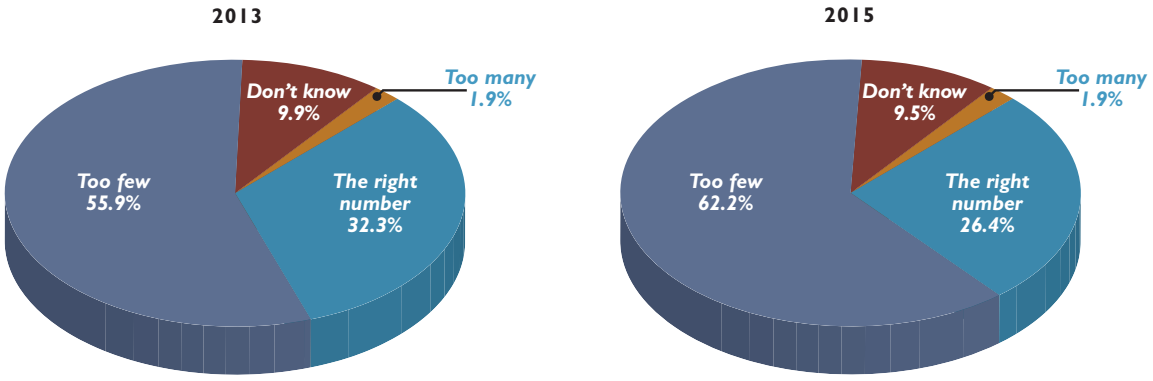
In examining shortages across industry verticals, the greatest shortages are reported in healthcare and education. While still significant, the workforce shortage is the least in the Information Technology industry vertical. However, over half of IT security professionals report that their organizations have too few information security professionals.

Too Few Security Workers by Industry Vertical (Percent of survey respondents in each industry vertical)

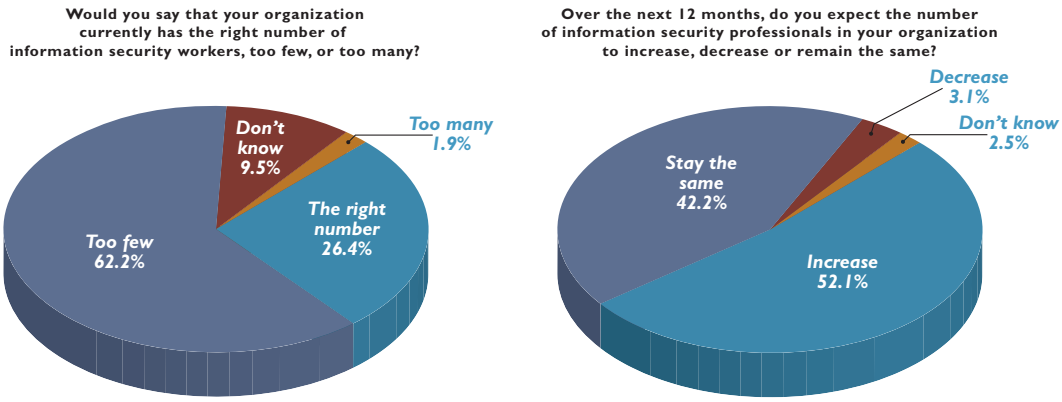


This shortage is hardly static. In comparing survey-over-survey results, the shortage worsens. In 2013, the percentage of security professionals reporting "too few" information security professionals was 55.9%, 6.3 percentage points lower than the 2015 survey.

Would you say that your organization currently has the right number of information security workers, too few, or too many?

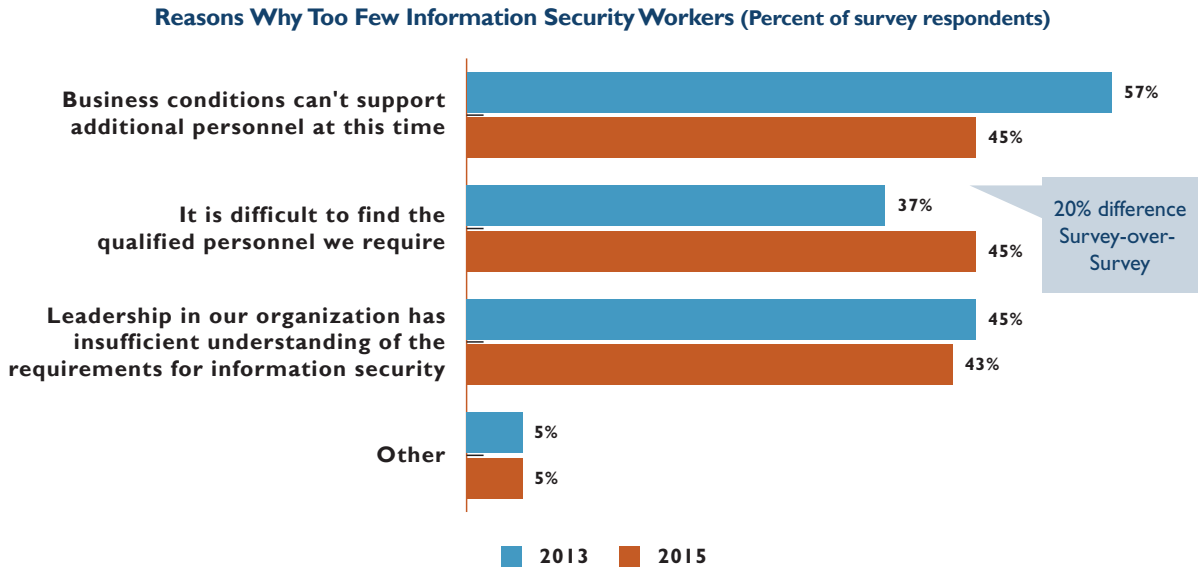


Intuitively, the growing gap is easy to explain. The assumption would be that the number of security professionals being hired is less than the number needed. The results of the 2015 study support the assumption. In fact, the difference between organizations hiring and those that have too few security workers is 10 percentage points. As shown in the charts below, 62% of survey respondents state too few information security workers versus 52% projecting an increase in information security professionals.



The reason for a lack of security professionals is as one might expect. In 2013, the number one reason was "business conditions can't support additional personnel at this time," just edging out "it is difficult to find the qualified personnel we require." "Leadership in our organization has insufficient understanding of the requirement for information security" rounds out the top three reasons.

When comparing the results of the 2013 survey to the 2015 survey, a transformation has occurred. In 2013, 57% of respondents believed that business conditions could not support additional personnel, a full 20 percentage points higher than the 37% who believed it was difficult to find the qualified personnel required. In 2015, these same two reasons received equal selection percentages by the survey respondents.The dramatic shift from funding to finding qualified personnel is another datum reinforcing the theme of a shortage of security professionals.



Workforce Size Estimate and Projection

A perfect storm is enveloping the information security workforce with the resulting wake being a widening gap between the number of security professionals needed and the actual number available to be hired. Unfortunately, reducing this gap will be fraught with challenges as the factors contributing to both the growing need and constrained hiring are numerous and, in many ways, structural. Therefore, the remedy is neither a silver bullet nor immediate.

As previously illuminated, the demand for security professionals will continue to escalate. Prominent drivers in this escalation include the following:

- **Evasive cyber threats** – The rising sophistication of cyber threats is not just to accomplish a singular goal (e.g., steal sensitive information), but to be persistent and effective over an extended period of time. To accomplish these objectives, evading detection and, if detected, silently adapting to either continue or reappear later are part of the hacker's operating principles. Consequently, identifying compromises and qualifying their severity requires constant diligence and deep pockets of expertise. An advanced degree of talent, knowledge, and time is also required to thoroughly root out discovered compromises.

- **Larger IT footprints** – The growing ubiquity of mobile devices used for business, both corporate-issued and personally owned, and the increasing adoption of cloud services contributes to a larger IT footprint to protect. Adding to the complexity of this spreading footprint and subsequently the effort required to protect it are the swirling varieties of mobile devices (manufacturers, operating systems, and models) and cloud environments (service models and providers).

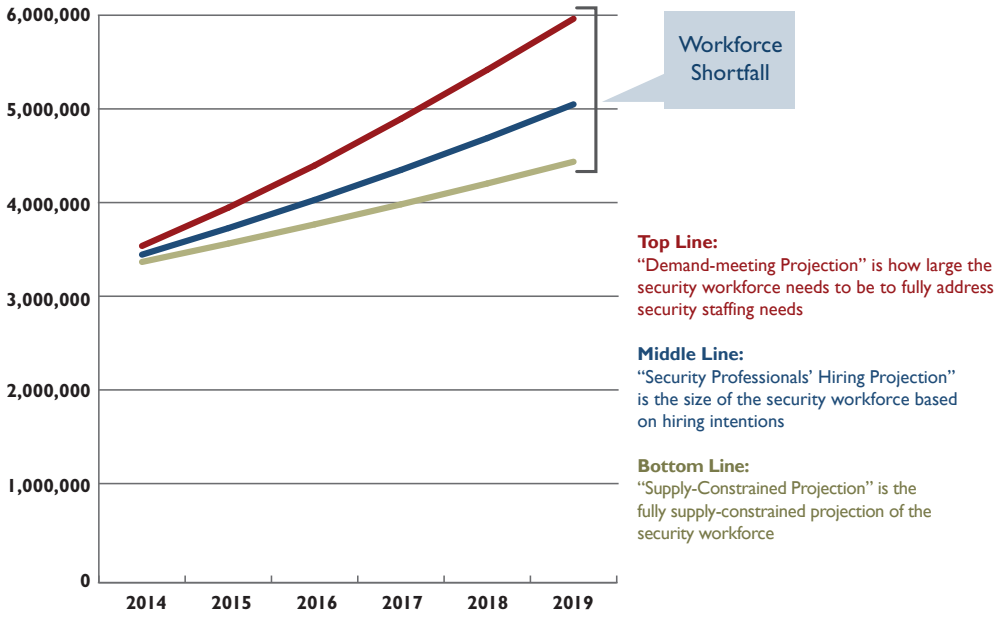
- **More security technologies** – Evasiveness of threats and a growing IT footprint require next-generation security technologies to replace and supplement in-place technologies. With this, the security operations group has more dashboards to view, dials to turn, and alerts and reports to examine. Furthermore, expertise in effectively and efficiently managing a growing stable of security technologies does not materialize overnight; investment in formal and on-the-job training is required. Having a portion of the security staff active in some form of training and education, thus taken off-line, at any point in time is increasingly a common necessity.

- **Self-inflicted wounds** – No one is perfect and perfection cannot be expected in an IT world of perpetual change. Configuration errors and oversights have and will continue to occur. Similarly, end users will have lapses in judgement (e.g., click on an untrusted link). Collectively, re-do and recovery are also a routine part of security professionals' activities. Also and equally important, the frequency of vulnerability scanning, a primary means to reduce vulnerabilities during and after software development, does not match the perennial top-rated security concern of application vulnerabilities. While reasons abound for this mismatch, the end result remains unchanged: additional and mostly reactionary security effort.

Recruiting and on-boarding new security professionals present their own sets of challenges. First, evidence of a tightening labor market is omnipresent—rising wages, persistently high employment levels, and increasing employee churn. Subsequently, approval to hire is no guarantee that candidates will line-up. Second, a tight labor market exerts downward pressure on the skill and experience levels that will be accepted. With fewer candidates, acquiring the "perfectly matched" candidate fades in likelihood. This, in turn, contributes to longer training and indoctrination periods for new hires in order for them to reach the productivity levels of existing staff. Correspondingly, an organization's capacity to on-board new hires is constrained; only so many can pass through the gateways at one time, and staging hiring over longer periods of time becomes an inescapable reality. Finally, in economic terms, higher wages strain an organization's base of justification for expanding its security teams. Accepting the risks associated with a less-than-preferred security posture due to fewer security professionals becomes a more attractive alternative over exponential or even linear additions to existing security teams.

In consideration of these demand-and-supply factors that are at play in the information security workforce and armed with new questions in the 2015 survey on organizations' hiring intentions, Frost & Sullivan is equipped, for the first time, to not only project the workforce size needed to effectively address the security challenges now and in the future (i.e., supply matching demand), but also estimate the size of the information security workforce in full consideration of workforce supply constraints. The difference between these two series represents the workforce shortfall or gap.

Projected Information Security Workers Globally



Thousands	2014	2015	2016	2017	2018	2019	2014-2019 CAGR
Demand-Meeting Projection	3,568	3,972	4,416	4,908	5,424	5,963	10.8%
Security Professionals' Hiring Projection	3,477	3,756	4,053	4,369	4,706	5,061	7.8%
Supply-Constrained Projection	3,400	3,593	3,796	4,007	4,227	4,456	5.6%
Shortfall	**168**	**378**	**621**	**901**	**1,172**	**1,536**	

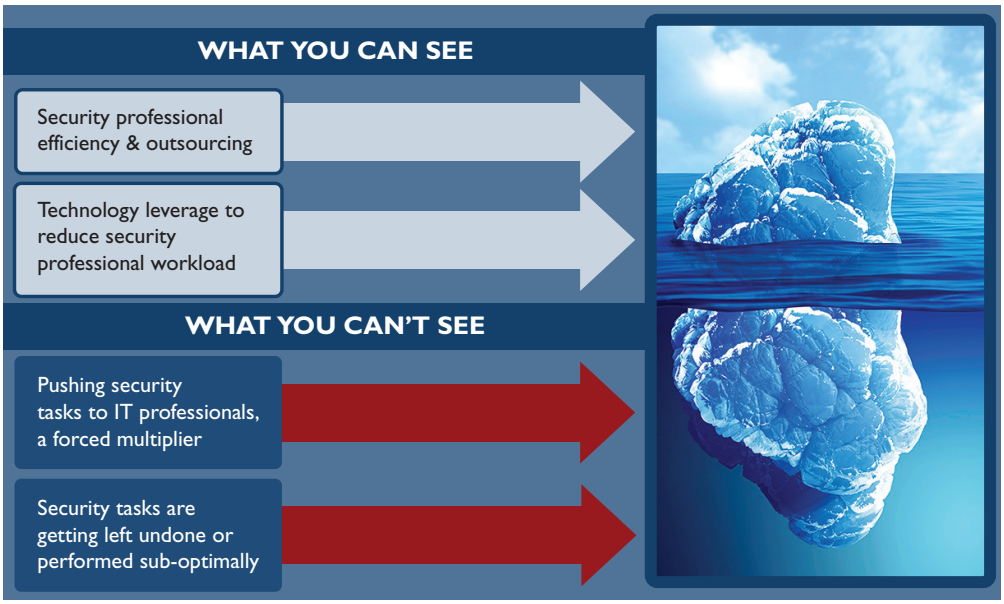
This next table presents the workforce projections by region. For the supply-constrained projection, the Americas region leads in both workforce size and growth rate, reaching 1.9 million security professionals in 2019 with a corresponding compound annual growth rate (CAGR) of 6.0% over five years.

Security Professional Workforce by Region

Thousands	2014	2015	2016	2017	2018	2019	2014-2019 CAGR
Demand-Meeting Projection							
Americas	1,495	1,673	1,867	2,081	2,308	2,546	11.2%
EMEA	995	1,108	1,230	1,363	1,502	1,646	10.6%
APAC	1,079	1,191	1,320	1,463	1,614	1,771	10.4%
Total	**3,568**	**3,972**	**4,416**	**4,908**	**5,424**	**5,963**	**10.8%**
Supply-Constrained Projection							
Americas	1,418	1,505	1,596	1,692	1,792	1,897	6.0%
EMEA	956	1,013	1,072	1,134	1,200	1,267	5.8%
APAC	1,026	1,076	1,127	1,180	1,235	1,292	4.7%
Total	**3,400**	**3,593**	**3,796**	**4,007**	**4,227**	**4,456**	**5.6%**

The impacts of the information security workforce shortfall are both seen and unseen. Stimulating greater efficiency from security professionals, outsourcing, and increasing technology leverage are visible trends. Pushing security tasks onto traditionally non-security IT professionals and leaving some security tasks undone or sub-optimally completed are the larger, unseen outcomes.

The Impacts of the Security Professional Workforce Shortfall



Security professionals feel that the workforce shortage has its greatest impact on the existing information security workforce. The next most significant impact is on the organizations as a whole.

What is the impact of your organization's shortage of information security workers on each of the following?
(Selected as Top 2 on a 5-point, Very-Great-Impact-to-No-Impact-at-All Scale)

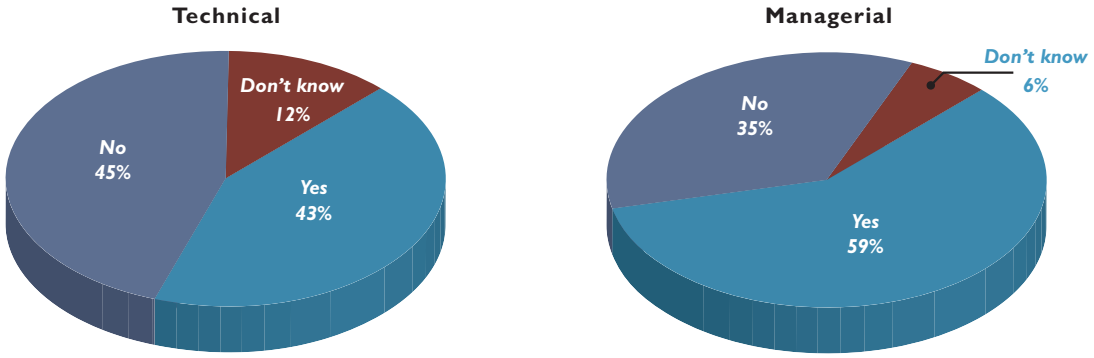
Train and Retain

Given the issues that have been articulated with respect to recruiting qualified security professionals, retaining existing security professionals becomes especially important. The top two initiatives for retaining security professionals are training related. Improving compensation lands at the third spot on the list, further emphasizing the importance of training. Interestingly, the fourth and fifth most commonly rated as "very important" are flexible work schedules and flexible working arrangements, suggesting that employers can improve retention with initiatives that do not have a significant expense-line impact.

How important are each of the following initiatives for the retention of information security professionals at your organization? (Percent selected as very important)

Whether adequate resources for training and professional development opportunities exist seems to be an area of differing opinions. The majority of survey respondents in managerial roles, 59%, feel that there are opportunities, with 6% unsure. Survey respondents in technical roles, however, are less certain, with only 43% feeling adequate resources for training and professional development are available, with 12% unsure.

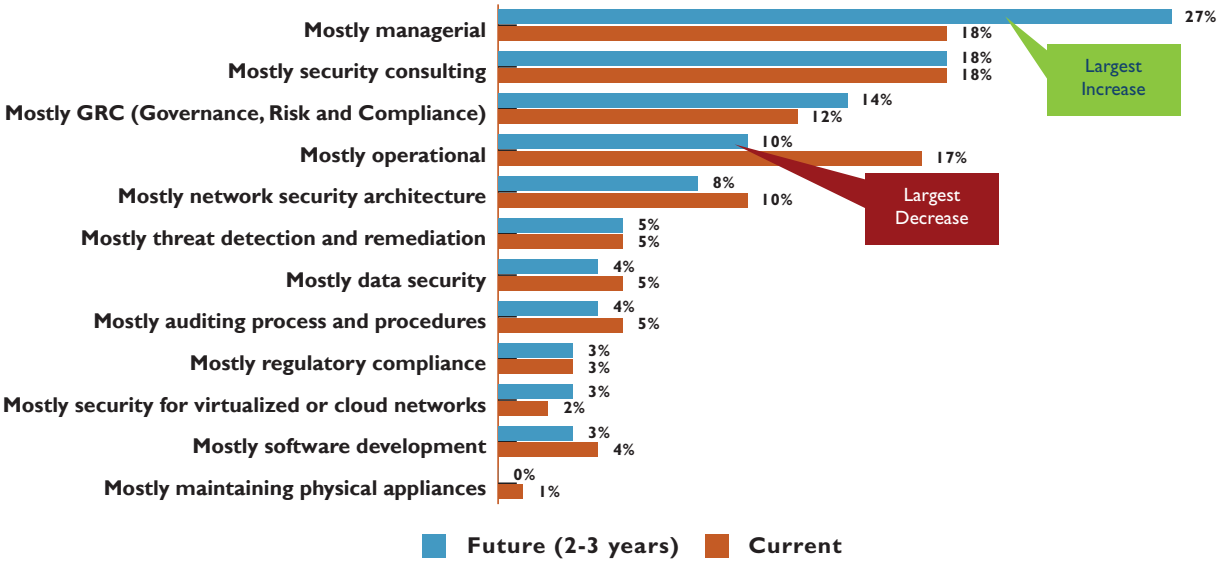
Does your organization provide adequate resources for training and professional development opportunities for your information security workforce? (Percent of survey respondents by job role)



Training of the Right Role

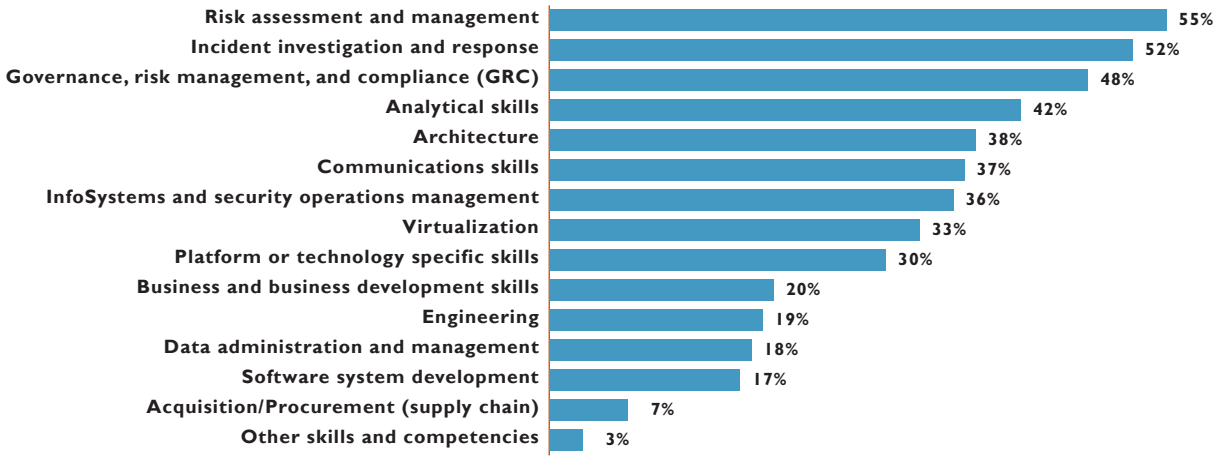
The objective of training is to prepare a person for future roles. The results from the study show that security professionals are ambitious and show a proclivity for investing in their professional development. Naturally, as security professionals project their roles two to three years into the future, many security professionals in operations roles do not see themselves in that same role in the future. Additionally, many that are currently not in managerial roles see themselves in managerial roles in the future.

Security Professional Roles, Now and in the Future (Percent of Survey Respondents)



Although a significant number of security professionals see themselves moving into managerial roles, the skills and competencies that they look to acquire appear to very task related, not necessarily geared toward preparation for managing people or functions. For example, "business and business development skills" finds itself at number 10 on the list of skills and competencies to acquire. Clearly, a managerial role changes a security professional's task focus to be increasingly strategic with focus on coordinating and overseeing security initiatives tied to the goals of the organization. Understanding organizations and being able to communicate to senior management in return-on-investment (ROI) terms is critical to success for cybersecurity management. As security professionals advance in organizational roles, their educational investments also need to evolve to ensure professional success.

What are the skills and competencies that you will need to acquire or strengthen to be in position to respond to the threat landscape over the next three years? (Percent of Survey Respondents)



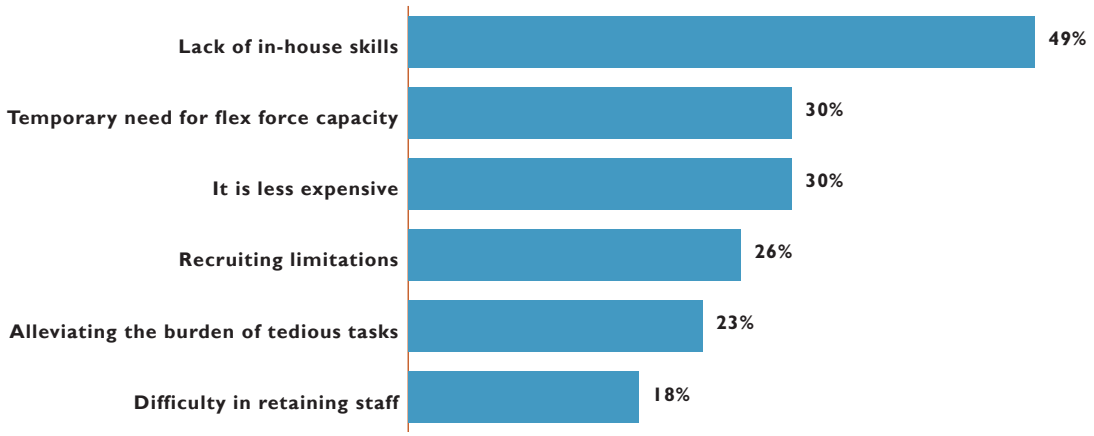
Invest to Improve: External Resources

Earlier in this study, we noted that increased spending on managed or outsourced security services and professional security services was projected by 30% and 27%, respectively, of the survey respondents. This approach is certainly one approach that leverages the availability and expertise of outside resources. Another approach is to increase the use of cloud services. Both approaches will be examined in this section.

Managed Security Services

Whether outsourcing a portion of ongoing security operations to a managed security service provider or engaging a professional security service provider for a bounded project (i.e., project end defined by contract), the reasons are similar. As shown below, shortages in needed skills or personnel underlie these reasons. Additionally, 29% of survey respondents indicated that outsourcing was somewhat or very likely a strategy their organizations will employ to combat security technology sprawl.

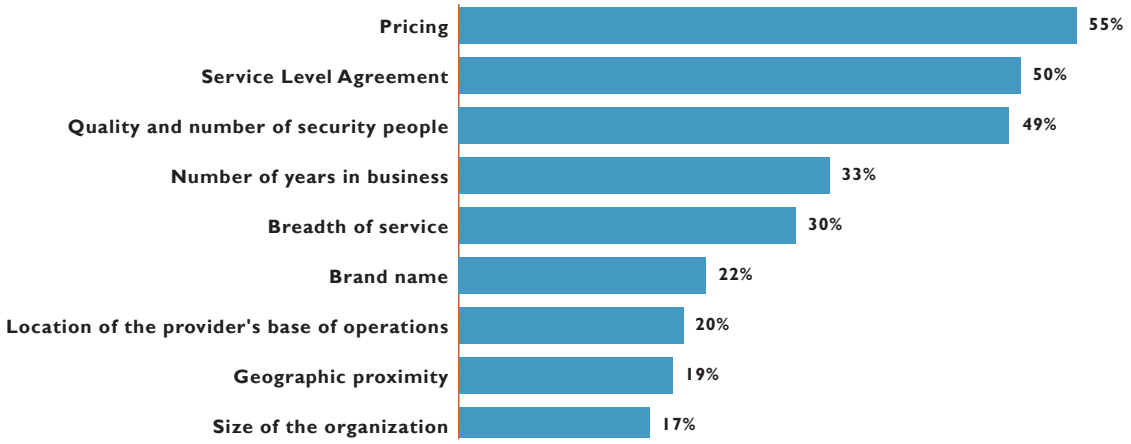
Reasons for Outsourcing (Percent of Survey Respondents at Organizations that Outsource)



Correspondingly, survey findings also show that outsourcing is more to augment existing internal security teams than to replace. Of the survey respondents that projected an increase in spending in managed security services or professional security services, a majority also projected spending more on personnel over the next 12 months. Furthermore, projected reductions in personnel spending were cited by 4% or less of the survey respondents projecting an increase in managed or professional security services.

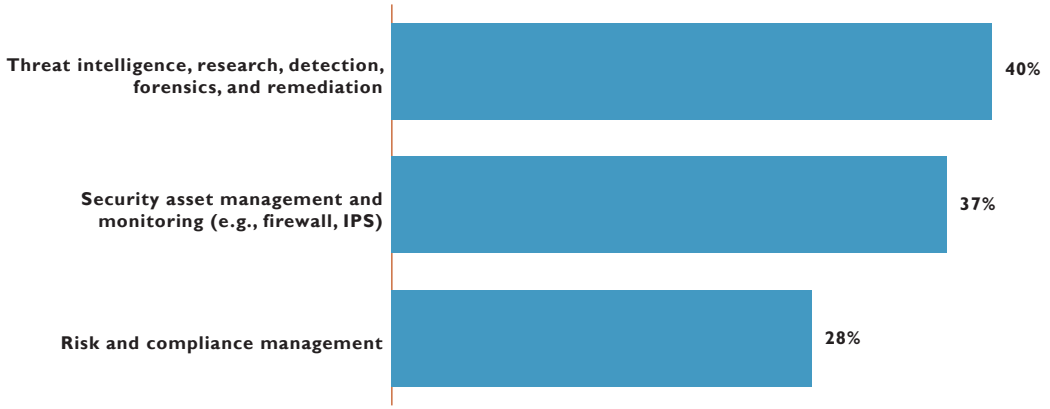
When asked about the criteria in selecting a managed or professional security services provider, three criteria stood out above all others, as shown in the chart that follows. Together, the meaning is clear: organizations want security services providers that are capable, contractually back up those capabilities, and service pricing demonstrates the provider's attentiveness to cost efficiency and operational proficiency.

Criteria in Selecting a Managed or Professional Security Services Provider
(Percent of Survey Respondents at Organizations that Outsource)

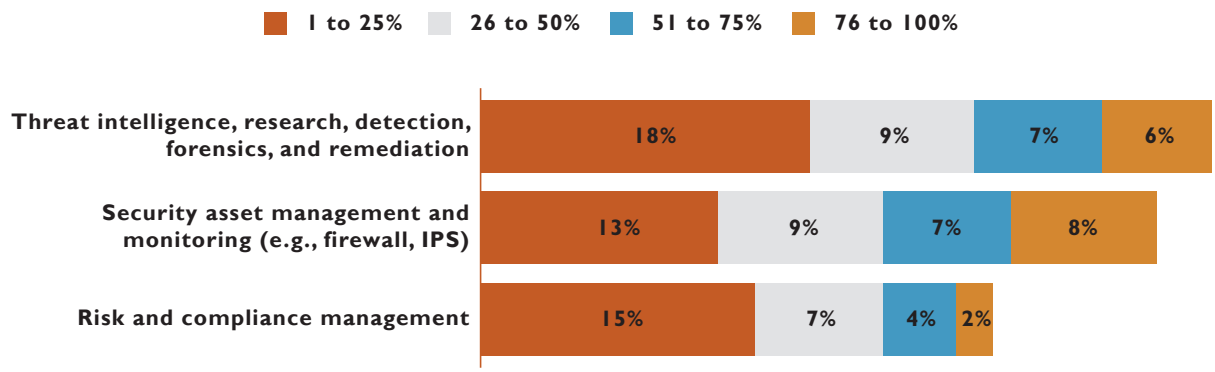


The next three charts show the principal outsourced security operations, the portion of those operations that are outsourced, and the projected change in spending over the next 12 months. Considering that survey respondents stressed an increasing need to improve threat detection and rising adoption of advanced analytics with the related need for specialized skills and training, the slightly higher use of the outsourced services category that includes threat intelligence and detection is logical. Plus, most managed security services providers highlight their multiple sources of threat intelligence as assets in serving their customers (i.e., they see and process more bytes of information than their customers possibly can).

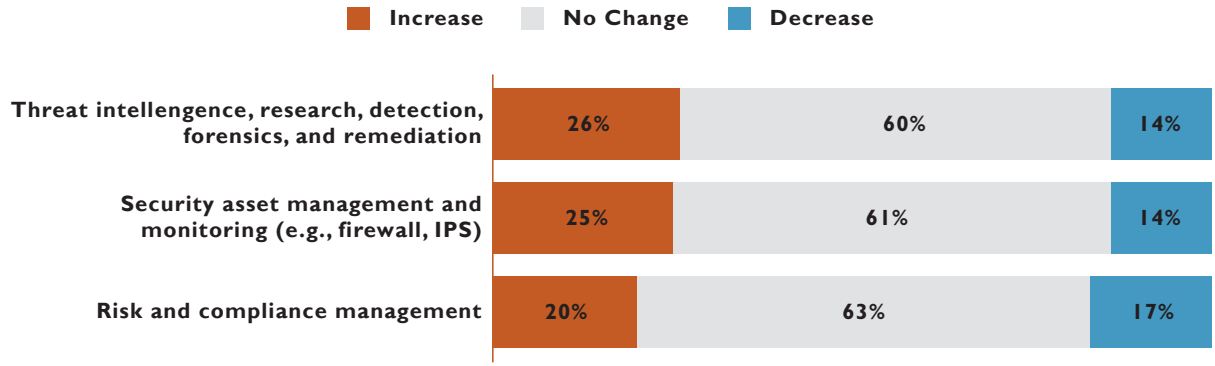
Outsourced Security Operations (Percent of Respondents in Organizations that Outsource)



Portion of Security Operations Currently Outsourced (Percent of Respondents in Organizations that Outsource)

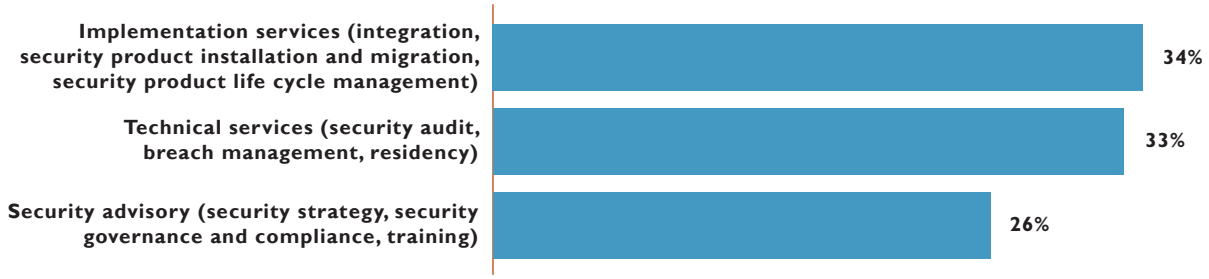


Projected Change in Outsourced Security Operations over Next 12 Months (Percent of Respondents in Organizations that Outsource)

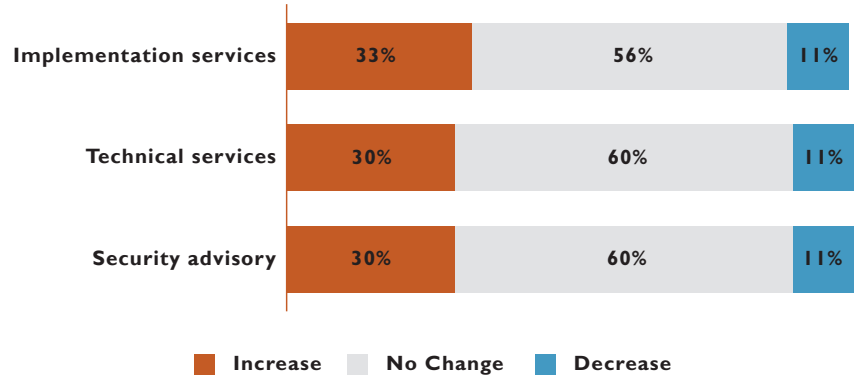


Of professional security services, implementation and technical services are statistically equivalent in current use among the survey respondents and in the projected change in spending.

Current Use of Professional Security Services (Percent of Survey Respondents in Organizations that Use Professional Services)



Projected Change in Professional Security Services over Next 12 Months (Percent of Survey Respondents in Organizations that Use Professional Services)

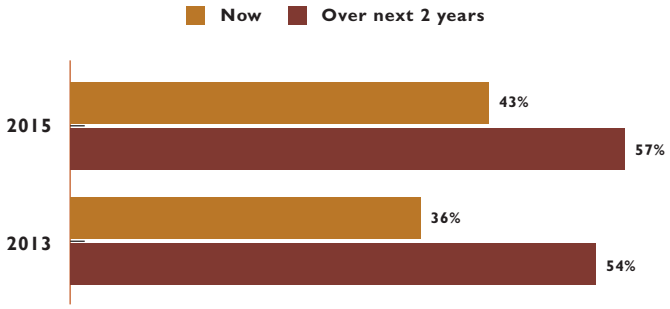


Cloud Services

The reason for including cloud services in this external resources category is that cloud services are a form of outsourcing. At minimum, the cloud provider has implicit responsibility for securing the physical resources that underlie the cloud services (e.g., data center and servers). This implicit security responsibility increases further up the layers of software (e.g., virtualization layer, operating system, and application) as cloud services move from platform as a service (PaaS) up to software as a service (SaaS). Correspondingly, the more security responsibilities that the cloud provider has, the less that are the responsibility of its customers; that is, a transfer of responsibility or outsourcing.

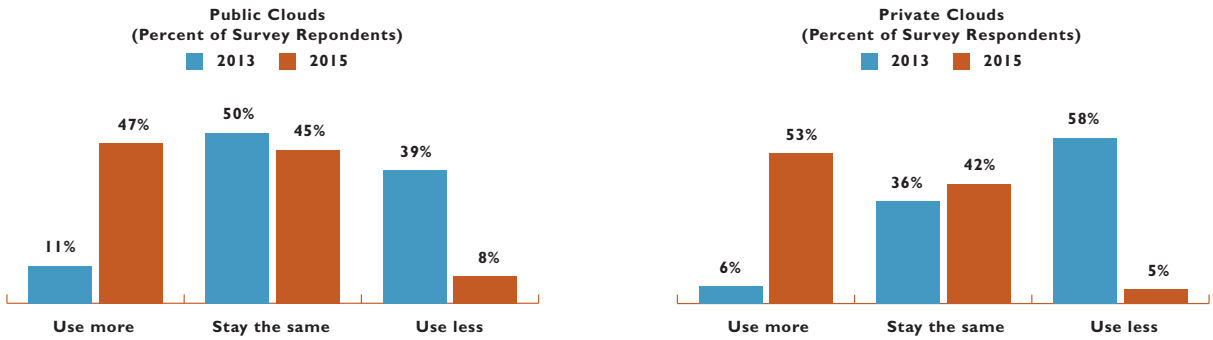
For many organizations, cloud adoption is no longer a question of if, but how much. In sequential surveys, security professionals confirmed that the cloud's priority for their organizations is on the rise.

Cloud Computing Priority (Percent of Survey Respondents Choosing Top or High Priority)



Furthermore and in a significant reversal in information security professionals' views on the future use of cloud services by their organizations, a significantly higher percent of respondents stated cloud usage would increase over the next two to three years in the 2015 survey versus the 2013 survey. A similar percentage flip occurred with a reduction in cloud usage.

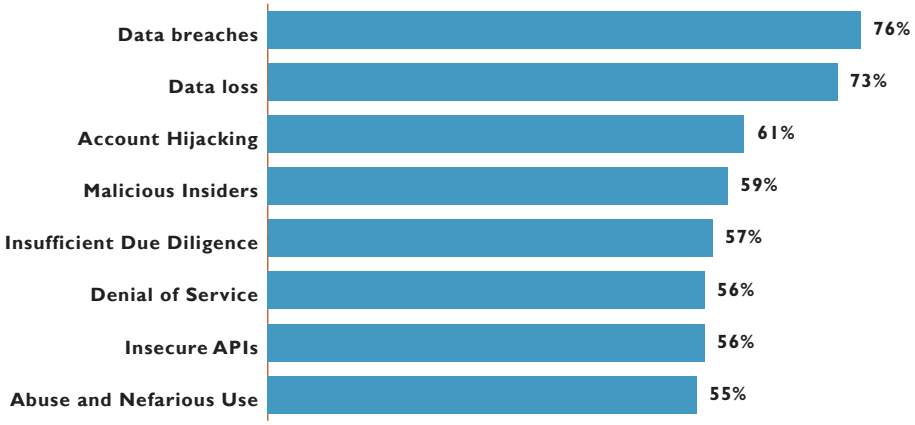
Public Clouds and Private Clouds (Percent of Survey Respondents)



A similar survey finding is present when looking at future use of the cloud by service type. In the 2015 survey, 43% of survey respondents stated PaaS usage would increase, 46% for IaaS, and 52% for SaaS.

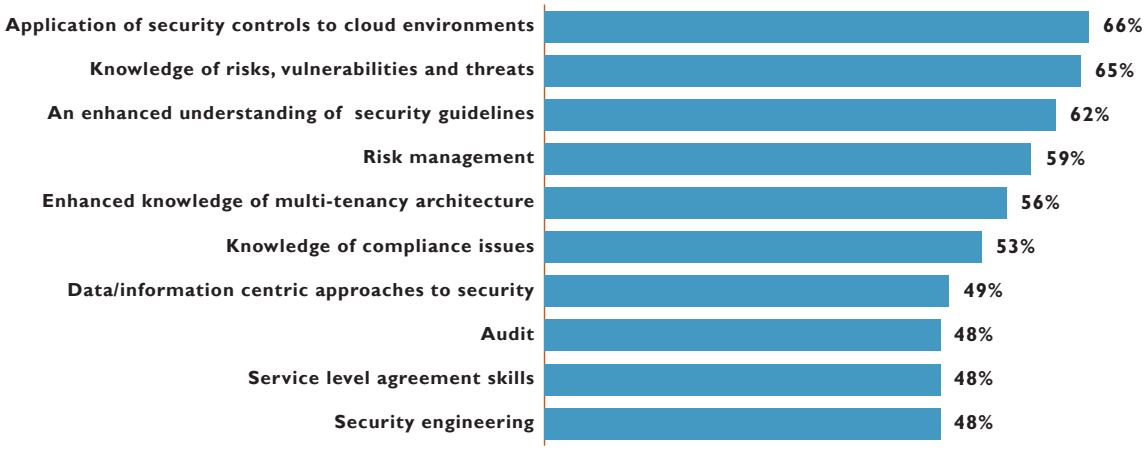
This rising priority and use of cloud services does not, however, materialize in a similar reduction in security concerns surrounding cloud services. Placed into the context of the Cloud Security Alliance's "Notorious 9 Security Threats," the survey respondents indicated their level of concern for each threat. Data breaches and data loss topped the list of concerns.

Cloud Security Alliance's Cloud Security Threats (Percent of Survey Respondents Choosing Top or High Concern)



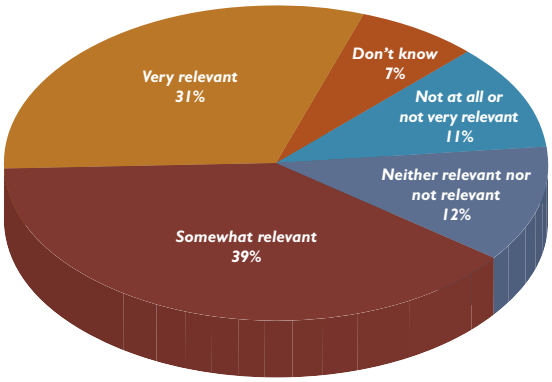
Closing this divide between increasing cloud adoption but high levels of security concerns will require specialized skills in cloud security. According to the survey, 73% of the survey respondents indicated that new security skills will be required. Specifically on the skills needed, survey respondents indicated the following.

Skills Needed For Cloud (Top 10 Selections by Survey Respondents)



Last, the need for new cloud security skills must be coupled with a means to acquire and prove competency in those skills. To that, the survey respondents were very much in favor of a cloud security and certification program; 70% view such as program as somewhat or very relevant.

Relevance of Cloud Security Certification (Percent of Survey Respondents)



THE LAST WORD

The 2015 Global Information Security Workforce Study is rich with insights that will help guide, prepare, and retain information security professionals. We trust that this white paper has articulated many of the key findings and you will find them valuable in preparing your organization's security workforce for the challenges ahead.

However, key messages elevate themselves above all others; a call to action if you will. The growth that we saw in the workforce since the 2013 study was below our expectations. The difference between our expectations from 2013 and the reality of 2015 was not due to a lack of openings, as we clearly have seen that companies are finding budget for personnel less challenging. The difference is not due to a lack of need, as clearly the cybersecurity environment is more challenging than ever before. The difference is also not due to an unappealing work environment, as job satisfaction among information security professionals is as high as we have ever seen. The difference is due to a lack of qualified information security professionals entering the workforce.

Solving this issue is not going to be done by a single person or entity alone. Clearly, (ISC)² is dedicated to addressing this issue, but (ISC)²'s contributions will not be enough. Solving the problem will require the cooperation of not just the information security community, but also all cyber-enabled organizations to elevate the importance and ownership of security across all employees. This elevated importance will, in turn, drive greater interest in information security as a career choice.

Awareness needs to be increased about the advantages and benefits of a career in information security. The awareness needs not only be made to those within the information technology profession, but to potential information technology professionals—those still studying within the many quality academic institutions that prepare tomorrow's workforce. Only by attracting more to the security profession can the shortage of information security professionals be genuinely addressed.

Needless to say, a lack of action will aggravate the shortage. With a lack of action, finding qualified personnel will become more challenging and the salaries of information security professionals will continue to rise. Also, a lack of action will result in some security tasks not getting done or being done ineffectively or sub-optimally, resulting in unpalatable vulnerabilities in cyber defenses and an inefficiently run security department.

Similar to attracting new talent to the information security profession, IT community cooperation is needed to solve another cybersecurity problem. Consistent with past surveys, application vulnerabilities top the list of security professional concerns, and this concern is trending upward as a larger percentage of survey respondents selected this vulnerability either as a top or high concern than in previous surveys. The era of viewing "bolt-on security" as a panacea for application vulnerabilities needs to end. Instead, security needs to be integral to the process of software development, planned for and built in from the start. To address the issue, the entire IT community needs to come together and address the issue holistically. A demand will always exist for dedicated security professionals; however, a growing need also exists for IT professionals to have security proficiency and expertise. A community has enabled the growing problem, and a community will be needed to solve it as well.

As a concerted and collaborative effort across organizations and disciplines, a security workforce that can address the evolving needs and complexities of cybersecurity and usher in safe and secure cyber innovation is possible. This possibility, however, cannot wait. The time to act is clearly now.

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 over 100,000 members in more than 160 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 a non-profit charitable trust that aims to empower students, teachers and the general public to secure their online life by supporting cybersecurity education and awareness in the community, including industry research like the (ISC)² Global Information Security Workforce Study, through its programs and the efforts of its members. More information is available at www.isc2.org and www.isc2cares.org.

About the Research Partners

Booz Allen Hamilton is a leading provider of management consulting, technology, and engineering services to the US government in defense, intelligence, and civil markets, and to major corporations and not-for-profit organizations. Booz Allen is headquartered in McLean, Virginia, employs more than 22,000 people, and had revenue of $5.48 billion for the 12 months ended March 31, 2014. www.boozallen.com (NYSE: BAH)

NRI SecureTechnologies, a leading provider of information security solutions, is one of the group companies of Nomura Research Institute, Ltd. Established in 2000. It examines technology and business management aspects of information security at corporations, and offers a one-stop service from consulting to solution implementation, training, management and surveillance. http://www.nri-secure.com

Cyber 360 is a woman-owned company that specializes in the placement of Cybersecurity Professionals to commercial and government clients. With one of the largest networks of CyberPros in the U.S, they work with Cybersecurity Leaders, and their teams, struggling to hire skilled cyber professionals to secure their systems and reduce data and privacy risk. www.cyber360solutions.com

(ISC)² would like to acknowledge and thank CompTIA, Global Information Assurance Certification (GIAC) and Cybersecurity Challenge UK for their participation in the 2015 (ISC)² Global Information Security Workforce Study.

Auckland
Bahrain
Bangkok
Beijing
Bengaluru
Buenos Aires
Cape Town
Chennai
Colombo
Delhi/NCR
Detroit
Dubai
Frankfurt
Houston
Iskander Malaysia/Johor Bahru
Istanbul
Jakarta
Kolkata
Kuala Lumpur
London
Manhattan
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

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, TX 78229
Tel 210.348.1000
Fax 210.348.1003

London
4 Grosvenor Gardens
London SWIW 0DH
Tel +44 (0)20 7343 8383
Fax +44 (0)20 7730 3343

877.GoFrost
myfrost@frost.com
www.frost.com

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?

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