

# Women in Security: Wisely Positioned for the Future of InfoSec



F R O S T  S U L L I V A N

A Frost & Sullivan White Paper

Michael Suby, VP of Research

A Frost & Sullivan Market Study in Partnership with:



Booz | Allen | Hamilton  
strategy and technology consultants

- Executive Summary..... 3**
- Introduction ..... 4**
- Study Objective and Methodology ..... 4**
- Past and Current Gender Profiles ..... 5**
  - Salary Analysis..... 10*
- The Future of InfoSec ..... 13**
- Bridging the Workforce Shortage Gap ..... 16**
- The Last Word..... 18**
- Women in Security Research Review Panel..... 19**
- About (ISC)<sup>2</sup>® ..... 20**
- About the (ISC)<sup>2</sup>® Foundation ..... 20**
- About Booz Allen Hamilton..... 20**

## EXECUTIVE SUMMARY

According to (ISC)<sup>2</sup>'s most recent Global Information Security Workforce Study, women in the information security profession represent 10% of the workforce—a percentage that is unchanged from two years ago. Although their sheer numbers in this profession are increasing, they are only increasing at the pace of the profession as a whole.

The stagnant percent of women in InfoSec does not capture the changes under way in the InfoSec profession, where women are more significantly represented. In the most recent survey, one in five InfoSec women is in a governance, risk, and compliance (GRC) role. Comparatively for men, one in eight is in a GRC role. The context importance of this is twofold. First, the GRC role was, until the events of 9/11, a relatively obscure role in InfoSec. Now, however, not just women but also men recognize the rising importance of this role and other roles concentrated in managing business risk. Second, women, more than men, seized upon the growth opportunities in GRC early on. Thus, women as a percent in GRC roles is double their percent in all of InfoSec—20% versus 10%.

GRC and other risk management roles are not void of challenges. Prominent among the challenges are diffusing emotions, collaborating across multiple stakeholders, and adroitly balancing business objectives and risk management. Women, according to a survey-supplementing panel of InfoSec women leaders, are more likely to have these skills and have applied them in their successful careers, and view these skills as increasingly important as the InfoSec profession continues to grapple with the technical aspects of security operations while driving the InfoSec profession to be a more prominent strategic partner in business decision making.

Women also differ with men on how to address the widening InfoSec workforce shortage. While a shortage of qualified personnel was voiced by both women and men as a significant contributor, women stress the need to look beyond technical skills in hiring. This is not to discount the importance of technical skills; those skills remain important and women in InfoSec are converging on men in prominence of academic undergraduate majors in computer science and engineering. Rather, technical skills alone are insufficient in resolving the complex risk management dilemmas leaders in InfoSec confront now and in the future.

Women also stated in the survey that “buying” InfoSec talent through salary incentives is insufficient in addressing the workforce shortage. A mix of monetary and non-monetary incentives, such as flexible work arrangements, and varied training and education methods will be important in attracting and retaining the talent the InfoSec profession requires.

The InfoSec profession is changing with the times, it must. Women who have chosen InfoSec as a career recognize that change is needed. Also, by being opportunistic in their InfoSec careers, women are contributing to the evolution in the InfoSec profession. And, in doing so, their actions are positively affecting the hiring consideration of women in the InfoSec profession and, in turn, can reduce the workforce shortage. Yet, more can be done. Organizations can and should take action to promote the InfoSec profession among girls and women. Actions that can be taken include supporting cybersecurity education in primary schools, offering internships, pairing new InfoSec hires with mentors, and, as the survey described, adapting compensation plans and training to better align with the flexible working arrangements and diverse training options women expressed as important in retaining and engaging InfoSec professionals.

## INTRODUCTION<sup>1</sup>

The 2015 (ISC)<sup>2</sup> *Global Information Security Workforce Study* documented that the information security (InfoSec) profession is growing in numbers yet falling increasingly behind in meeting market demand. Furthermore, the complex demands on this profession have contributed to a workforce that is disproportionately older than 40 years old (70% are at least 40 years old versus less than 7% younger than 30 years old) and highly educated (more than 45% have either a Master's or Doctorate degree). At the same time, job satisfaction is quite high, with more than 75% stating that they are either somewhat or very satisfied, plus the surveyed InfoSec professionals expressed a strong proclivity to invest in their careers through a myriad training opportunities.

**InfoSec employment is also predominantly male. At approximately 10% of InfoSec professionals, attracting more women into the InfoSec profession would lessen the workforce shortfall.** Yet, as the Global Information Security Workforce Studies have illuminated, the proportion of women to men has been stubbornly stagnant. The number of women in information security employment is growing, but only at the rate of growth equal to that of the profession as a whole.

The aggregate numbers, however, mask the progress being made by women in the InfoSec profession. For instance, the undergraduate degrees of women in InfoSec are converging on those of their male counterparts. An increasing percent of InfoSec women have an undergraduate degree in either computer science or engineering, a noteworthy observation given the general affinity to hire people with similar backgrounds as the current workforce.

More interesting, however, is the path that women are taking once in the profession. Women are increasingly taking a career path that has a primary functional responsibility in governance, risk, and compliance (GRC). The Global Information Security Workforce Studies show that GRC is one of the growing InfoSec roles. Women, therefore, have positioned themselves wisely in an InfoSec profession that should not be defined by sheer headcount, but in the roles of those that are shaping the future practice of InfoSec.

In this paper, we describe gender differences within the InfoSec workforce based on surveys of InfoSec professionals sponsored by (ISC)<sup>2</sup> in partnership with Booz Allen Hamilton. In our analysis, we examined the survey results in three groups: (1) the total global survey, (2) leaders versus practitioners ("doers" was the term used in the 2013 paper on this same topic), and (3) survey respondents that selected GRC as their primary functional responsibility. Through a progression of examining smaller subgroups, homogeneity of the sample improves as does the robustness of the inferences (i.e., by minimizing the effects of exogenous factors such as cultural, economic, and locational). Additionally within this report, we interspersed perspectives from a panel of women leaders in the InfoSec profession.

## STUDY OBJECTIVE AND METHODOLOGY

This Women in Security white paper is based on the research emanating from (ISC)<sup>2</sup>'s Global Information Security Workforce Studies. The 2015 study is based on an online survey conducted over a four-month period starting in October 2014. The objective of that survey, and as presented in this study, is to gauge the opinions of InfoSec 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 InfoSec professionals. The diversity of survey respondents is reflected in the survey profiles, which can be found [here](#). As (ISC)<sup>2</sup> has conducted similar surveys in previous years, notable comparisons to the findings of the 2013 survey (12,396 survey respondents) are included.

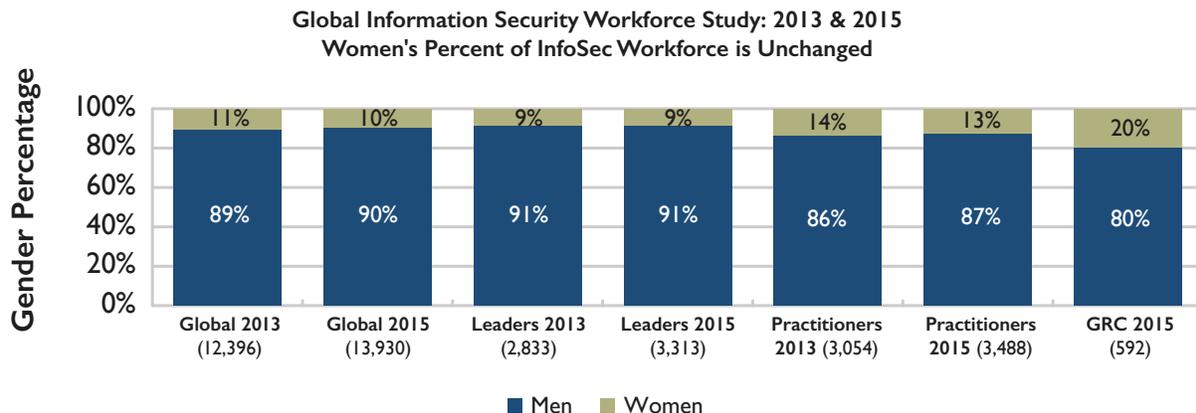
## PAST AND CURRENT GENDER PROFILES

As stated in the introduction, leaders and practitioners are two of the subgroups (i.e., a subset of the global survey) we examined. Included in these subgroups are survey respondents who have the following attributes:

- Located in a developed country
- Are employed in private industry
- Their employers have 500 or more employees

Leaders and practitioners are further defined by their job titles. Leaders include survey respondents with job titles of executives (CEO, CIO, CSO, and CISO), managers, architects, strategists, and strategic advisors. Practitioners include all the remaining job titles, with security analyst being the most prominent (24% of practitioners). The remaining subgroup, GRC, includes survey respondents that are employed in private industry, located in the United States, and selected GRC as their primary functional responsibility.

The percent of women in the InfoSec profession is essentially unchanged over the past two years, as shown in the chart below. Yet, what is apparent is that women represent a higher percentage in developed countries and their percentages vary based on primary functional responsibility. For example, one-fifth of women have a prominent GRC role (GRC was a new selection included in the 2015 survey). The numbers below in the parentheses reflect the number of survey respondents in the subgroups.



Placing these InfoSec gender percentages into a broader context, women are, in general, underrepresented in senior leadership and information technology roles. In terms of senior leadership, in a 2015 global survey of senior executives, an estimated 22% of senior leadership roles are held by women.<sup>2</sup> Regionally, there is material variation. Eastern Europe ranks the highest at 35% of senior leadership roles held by women. Developed APAC is the lowest region at 13%. The percent of women in senior leadership roles in North America and the European Union are 21% and 26%, respectively.

Of the specific leadership roles globally, this same survey determined that women are concentrated in support roles and have a very low representation in the chief information officer (CIO) role. Of the 22% of women in senior leadership roles, more than one-quarter of them (27%) are human resource directors. Only 9% hold the title of chief executive officer (CEO) and just 4% are CIOs.

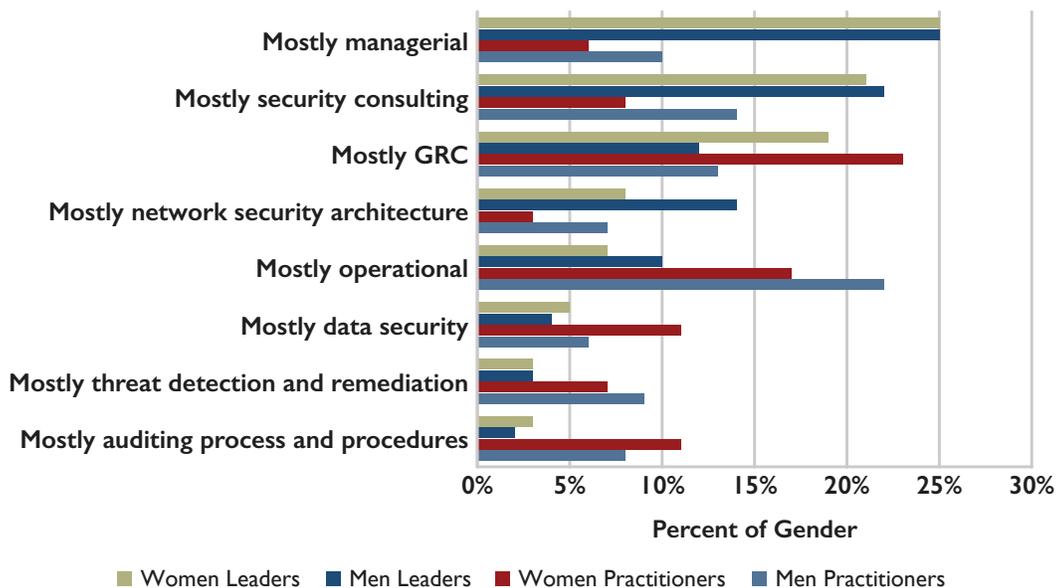
<sup>2</sup> *Women in Business: The Path to Leadership*

A similar decreasing percent of women exists in the United States when moving from total workforce to management and then to computer and mathematical occupations. The following 2014 averages from the US Bureau of Labor Statistics illustrate the decreasing percentages:<sup>3</sup>

| Occupation  | Women as a Percent of Total Employed |
|---|--------------------------------------|
| <b>Total, 16 years and over</b>   | 46.9%                                |
| <b>Management occupations</b>   | 38.6%                                |
| <i>Human resource managers (highest in management occupations category)</i>                     | 74.4%                                |
| <i>Computer and information systems managers</i>  | 26.7%                                |
| <i>Chief executives</i>   | 26.3%                                |
| <b>Computer and mathematical occupations</b>  | 25.6%                                |
| <i>Operations research analysts (highest in computer and mathematical occupations category)</i> | 55.4%                                |
| <i>Information security analysts</i>  | 18.1%                                |

Regarding differences between the genders in their primary functional responsibilities, a greater percent of women is in GRC roles than men (e.g., 19% of women leaders is in GRC roles versus 12% of men leaders). The opposite is the case for network security architecture and operational, as shown in the next chart.

2015 Global Information Security Workforce Study Repondents  
Women are More Concentrated in GRC Roles than Men



<sup>3</sup> Household Data Annual Averages; 11. Employed persons by detailed occupation, sex, race, and Hispanic or Latino ethnicity, 2014.

With regard to this prominence of women in GRC roles, the panel attributed this to women seizing the new opportunities that were emerging in GRC and pursued these opportunities to a greater extent than men. The following quotes reflect the perspective voiced by the panelists:



“9/11 was a catalyst that hit the US, where companies experienced tangible impacts related to security preparedness. Many organizations began assessing their preparedness and reflecting if information security was critical to their company’s resilience, causing many companies to elevate the role of the cyber security professional,” said Julie Talbot-Hubbard, associate vice president for IT Engineering, Infrastructure & Operations at Nationwide. “I assumed a GCR/continuity planning role at a prior employer due to the need and lack of interest.”

Renee Hodder, Information Risk Management consultant, Nationwide Mutual Insurance Company, added, “That’s a common theme. At a previous company, I got my feet wet with PCI because nobody was interested in leading that function. People had to get dragged into it. A mindset shift had to happen from ‘doing it because we have to’ (compliance) to ‘it’s the right thing to do’ (security). Leading that mindset shift was both a challenge and a career opportunity.”



Yet seizing on a growth opportunity in InfoSec alone is insufficient to spell success. The panel provided context on why women have been and will continue to be successful in GRC and other roles that are heavily concentrated in risk management.

Talbot-Hubbard stated, “Women’s natural tendency is to collaborate, bring teams together and to connect the dots and gain the trust of a diverse set of teams throughout the enterprise.”

Alice Fakir, executive director at Morgan Stanley, provided this synopsis on her rise in InfoSec, “I began my career as the only female on an engineering team. I saw an opportunity that no one else saw or wanted: document the systems and processes we were developing. Taking on that role led to additional work in project management, which led to being the lead client manager, which led to a successful career in InfoSec consulting.”

Both age and tenure in InfoSec are increasing for women and men in the full study and in each of the subgroups. Shown in the table below are the percent of survey respondents in the tails of the age and tenure brackets. The averages for the leaders and practitioners subgroups are also presented. With an average starting age in the InfoSec profession of approximately 30 years old (the difference between the age average and tenure average), the conclusion is the same regardless of gender: growth in the InfoSec profession in private industry is not coming from an upswing in younger talent, but rather a combination of retention of experienced personnel and an influx of personnel from outside InfoSec or from government (including military) InfoSec positions.

| Distribution of Gender in Age and InfoSec Tenure | Women Leaders |      | Men Leaders |      | Women Practitioners |      | Men Practitioners |      |
|--|---------------|------|-------------|------|---------------------|------|-------------------|------|
|  | 2013          | 2015 | 2013        | 2015 | 2013                | 2015 | 2013              | 2015 |
| <b>Age</b>                                       |               |      |             |      |                     |      |                   |      |
| % less than 30 years                             | 4%            | 4%   | 3%          | 2%   | 6%                  | 5%   | 6%                | 6%   |
| % 50 years or older                              | 36%           | 43%  | 26%         | 29%  | 35%                 | 34%  | 25%               | 26%  |
| <b>Average Age</b>                               | 45.7          | 46.7 | 43.7        | 44.6 | 44.4                | 44.7 | 42.8              | 43.0 |
| <b>Tenure in InfoSec</b>                         |               |      |             |      |                     |      |                   |      |
| % with 3 years or less                           | 3%            | 3%   | 3%          | 2%   | 6%                  | 6%   | 5%                | 7%   |
| % with 16 years or more                          | 31%           | 35%  | 30%         | 36%  | 27%                 | 27%  | 26%               | 28%  |
| <b>Average InfoSec Tenure</b>                    | 13.4          | 14.4 | 13.7        | 14.5 | 12.4                | 12.5 | 12.5              | 12.7 |

The industries where the genders are employed vary only modestly in the full study population and the subgroups. Of women, a higher percent of them are employed in healthcare than men. Conversely and of equal difference (approximately three percentage points), a higher percent of men are employed by information technology companies than are women.

Academic achievement is a characteristic of material difference between genders. The percent of women with either a Master’s or Doctorate degree exceeds the percent of men. For example, of women leaders, 58% have advanced degrees versus 47% of men. Both genders, as shown in the chart below, gained in percentages with advanced degrees since 2013; another inference that the InfoSec profession requires, attracts, or likely a combination of both, individuals of high academic achievement.



In terms of undergraduate majors from the global study, the InfoSec profession is dominated by three: computer and information sciences (49%); engineering and engineering technologies (20%); and business (10%). This same concentration pattern is present in the subgroups. What is noteworthy is the convergence between the genders. While men have a consistent distribution survey over survey, the percent of women with undergraduate degrees in computer science and engineering is increasing. Women migrating from other disciplines or from the government is a likely contributor to this shift.

| Percent of Gender in Top 3 Undergraduate Majors | Women Leaders |      | Men Leaders |      | Women Practitioners |      | Men Practitioners |      |
|---|---------------|------|-------------|------|---------------------|------|-------------------|------|
|   | 2013          | 2015 | 2013        | 2015 | 2013                | 2015 | 2013              | 2015 |
| <b>Computer and information sciences</b>        | 35%           | 43%  | 45%         | 46%  | 43%                 | 42%  | 47%               | 49%  |
| <b>Engineering and engineering technologies</b> | 11%           | 14%  | 22%         | 23%  | 8%                  | 14%  | 18%               | 20%  |
| <b>Business</b>                                 | 21%           | 13%  | 13%         | 12%  | 18%                 | 13%  | 11%               | 12%  |

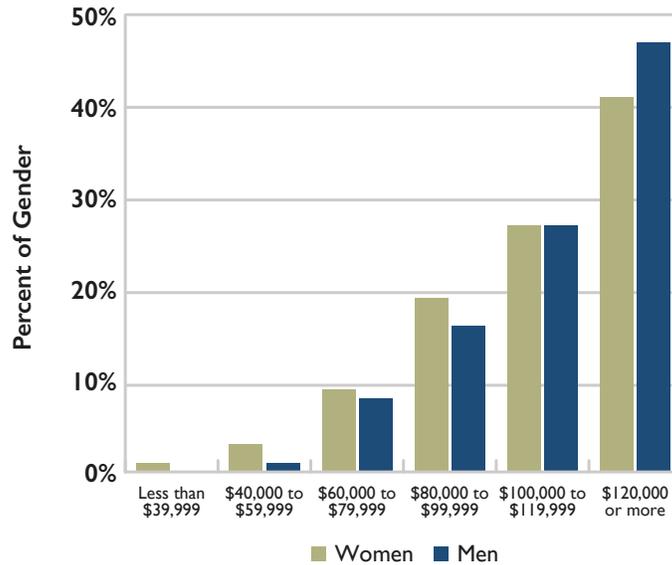
The mix of undergraduate majors based on the individual's primary functional responsibility does vary. For example, in the 2015 survey, 22% of women leaders in prominently GRC roles had a business degree versus 15% of men leaders with a prominent GRC role. Of practitioners, 18% of women and 18% of men in prominently GRC roles had a business undergraduate major. Correspondingly, the percent of both women and men in GRC roles with an engineering undergraduate major was less than the percentages show in the table above. The percentages for computer sciences had insignificant differences from the percentages in the table.

## Salary Analysis

To limit variables that can distort salary analysis, the narrowly defined subgroup of GRC was chosen. This subgroup is limited to respondents that are located in the United States, employed in private industry, and selected GRC as their primary functional responsibility. Beneficial in this analysis on women in security is that GRC is the primary functional responsibility with the highest concentration among women and, as will be shown in the next report section, a role of increasing prominence in InfoSec.

In this GRC subgroup, women’s average annual salary was 4.7% less than men (\$115,779 versus \$121,513). The distribution among salary ranges is similar between the genders with the largest exception in the \$120,000 or more bracket, where a higher percentage of men is represented than women (47% versus 41%).

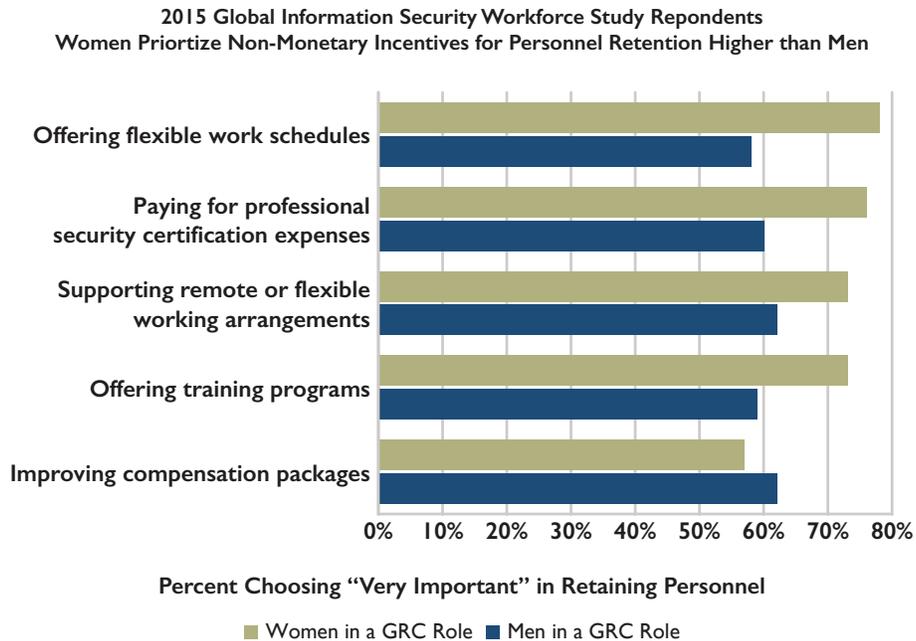
2015 Global Information Security Workforce Study Repondents  
Annual Salary Distribution of GRC Subgroup:  
A Smaller Percentage of Women are in the Highest Salary Bracket than Men



There are several contributing factors to men’s higher average annual salary in the GRC subgroup. Those factors include:

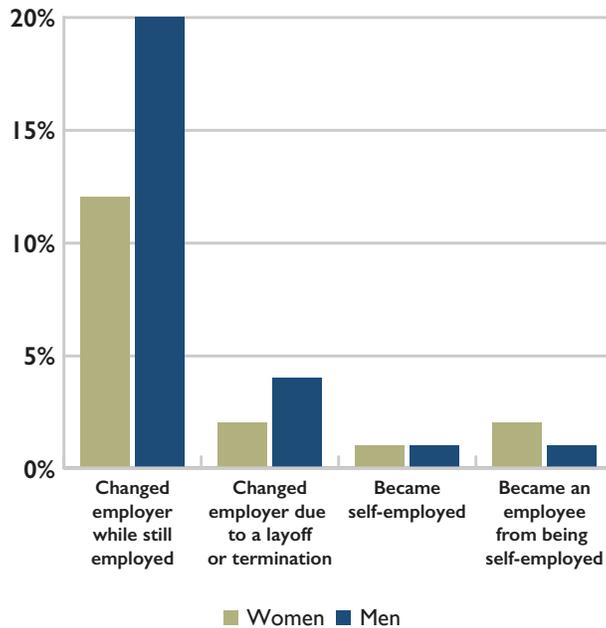
- Men’s average tenure in InfoSec is 5.6% longer than women (15.2 years versus 14.5 years)
- A smaller percent of men have a security analyst job title than women (21% versus 29%). The average annual salary for those with a security analyst job title (US only, private industry) is approximately \$95,000.
- Men place a higher emphasis on monetary compensation than other forms of work incentives than women, and are more aggressive in maximizing their monetary compensation. Both of these points are explored deeper in the following two charts.

Regarding emphasis on monetary compensation, the Global Information Security Workforce Study asked respondents what initiatives were important in retaining personnel. With the logical assumption that a survey respondent will project his or her opinions on what is important personally, not exclusively in the retention of others, the responses to this question can be inferred to mean “what is important to me.” From this perspective, the survey results show that women place higher emphasis on non-monetary incentives than men. Men placed only slightly more emphasis on monetary compensation than women, but indicated no non-monetary incentive had a higher importance.



This next chart on the GRC subgroup delves into the aggressiveness that the genders have in changing employers. Our implicit and logical assumption on this specific point is that the individual changed employers while still employed (the first set of vertical bars) in order to improve his or her career in some manner. As shown in this chart, a higher percent of men changed employers while still employed than women (20% versus 12%). In terms of no change in either employer or employment status in 2014 (not shown in the chart), 83% of women and 74% of men did not sustain an employer or employment status change.

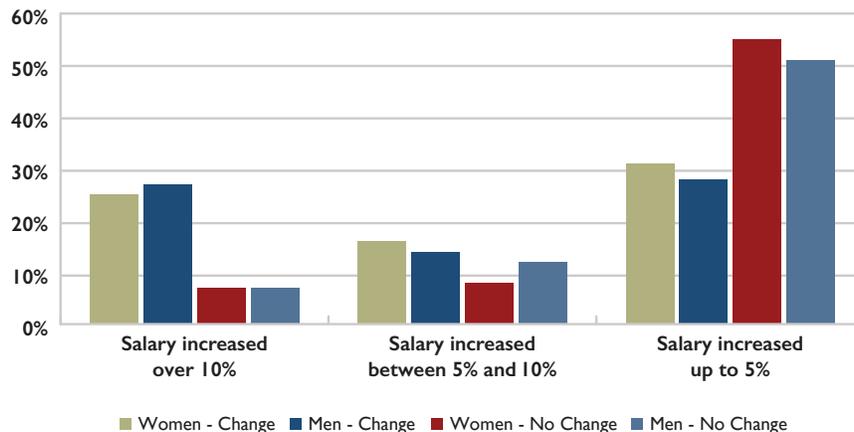
2015 Global Information Security Workforce Study Repondents  
 GRC Subgroup: Women Changed Employers Less Than Men



The next chart correlates the monetary benefits of changing employers while still employed (“Change”) versus having no change in employer or employment status (“No Change”). Please note that to increase the sample size to yield high-resolution results, the data for this chart encompasses all US-based InfoSec professionals employed in private industry, regardless of their primary functional responsibilities (i.e., not just GRC).

The inference from these results is that the greatest monetary rewards go to those that are willing to change employers. According to this survey data, a higher percent of individuals that changed employers while still employed received a larger year-over-year increase in salary than those that had no change in employer or employment status. Correlated with the previous chart, men, at least over the past year, reaped larger increases in salaries as they pursued new employment opportunities to a greater extent than women.

2015 Global Information Security Workforce Study Repondents  
 Changing Employer Improves Potential for a Larger Salary Increase



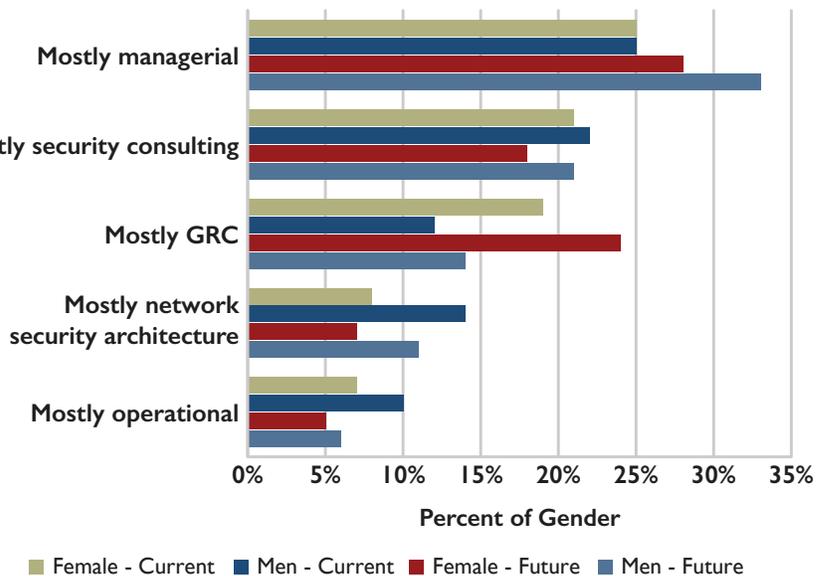
Separately, women in the GRC subgroup do have factors that may bolster their salaries relative to men. Those include: (1) a higher percent of women in prominent GRC roles has advanced college degrees versus men, and (2) women are more concentrated in the high-cost-of-living Washington, D.C., beltway states of Virginia and Maryland than men. The magnitude of these factors would require deeper analysis than the data allows. Yet, in the case of academic degrees, this factor likely diminishes with age and tenure as salary becomes more a function of in-career accomplishments than academic achievements. Furthermore, what can be confidently concluded is that these two factors are insufficient to offset the factors that contributed to a higher average salary for men.

## THE FUTURE OF INFOSEC

As is well known, the practice of InfoSec is one of adaptation. Cyber threats are constantly evolving and security risk continues to ramp upward due to numerous contributors, notably the broadening systemization and network accessibility of business operations. Therefore, an aspect of analysis on women in security requires an assessment on how the InfoSec profession intends to adapt. For this, we examine the viewpoints of respondents in the leaders subgroup on the changing complexion of primary functional responsibilities (i.e., currently and in two to three years) and the skills and competencies that will be needed to support this evolving mix of prominent InfoSec roles.

Shown in the chart below, women and men InfoSec leaders signaled similar directional viewpoints. Essentially, greater emphasis will be forthcoming in the managerial role and less in the operational and security consulting roles. In more functionally defined areas, GRC is expected to gain prominence, while network security architecture is expected to decline slightly. Combined, our broad takeaway is that InfoSec leaders are responding to the growing need to merge the practice of InfoSec deeper into managing business risk.

2015 Global Information Security Workforce Study Repondents  
For Leaders, Higher Future Prominence in the Management and GRC Roles is Predicted



The next chart displays the top six skills and competencies InfoSec leaders view as needed for the future. Consistent with the complexion of future roles, risk management, which we view as encompassing the top three categories, is where the InfoSec leaders of today view more skill development is needed over the next three years.



Our survey, as the panelists pointed out, did not capture all the skills and attributes needed now and in the future for leaders in the InfoSec profession. Two that the panelists singled out are emotional intelligence and the cornucopia of skills and insightfulness honed through childrearing.



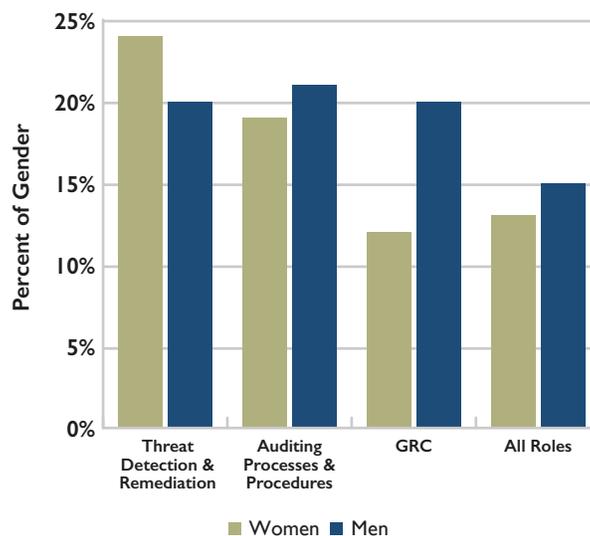
*“A common personality trait in this field is to want to be challenged, but men and women are challenged by different things,”* **Gurdeep Kaur, chief security architect at AIG,** *said. “Emotional Intelligence becomes more important beginning at the middle management level. It plays a big role in translating the dynamics (of people and technologies) that will impact the decision you make, that, in turn, impact risk management for an enterprise.”*

*“Being a mother of four kids and working has gained me the skills to multitask, prioritize and deal with stressful situations. Women that have kids know how to relate to people at any age and to diffuse touchy situations at home, bring everyone to the table, keep things calm while handling sensitive issues,”* **Karen Kabel, Operational Support and Security Technology Solutions manager at Great-West Life Assurance Company.** *“That’s exactly the skill set you need for a career in GRC and in security leadership.”*



As a side note on risk management skills, the market demand for InfoSec professionals with risk management skills is already here. The chart below shows the primary functional responsibilities with the highest rates of employer change, an indicator of “high-demand” roles. This sample includes all survey respondents that are located in the United States and employed in private industry.

2015 Global Information Security Workforce Study Repondents  
InfoSec Professionals in Risk Management Roles had the Highest Rate of Employer Change

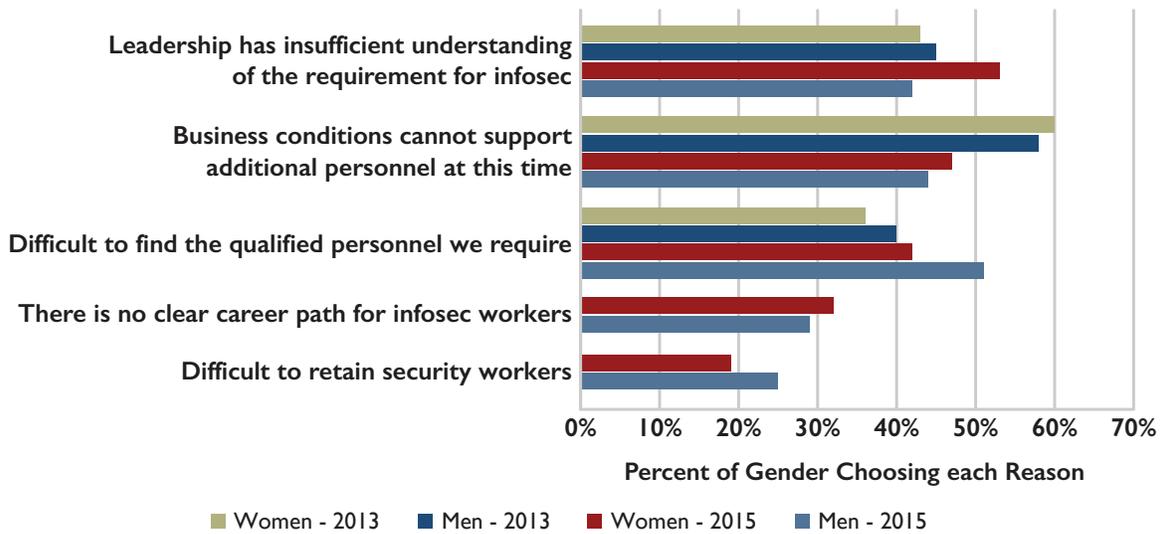


## BRIDGING THE WORKFORCE SHORTAGE GAP

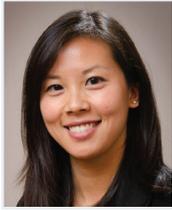
The workforce shortage in InfoSec is well documented in the (ISC)<sup>2</sup> 2015 Global Information Security Workforce Study and is projected to widen in the years ahead. The reasons for this shortage are multiple. However, there are differences of opinion between the genders on degree of influence.

Shown in the following chart are the five reasons survey respondents in the leaders subgroup chose as contributing to the shortage. Both genders expressed growing concern over the difficulty in finding qualified personnel, with men expressing the largest change survey over survey. Both genders also expressed equally proportionate easing of business conditions as a contributor. On material differences between the genders, a higher percentage of women view leadership as being an impediment versus the percentage of men. The bottom two contributors were new selections in the 2015 survey. Given the rising shortage and the previously highlighted double-digit rate of employer change, we expect the difficulty in retaining InfoSec professionals will become a growing contributor in the future. Related, women’s greater emphasis on receiving both monetary and non-monetary incentives to retain InfoSec professionals may prove to be a change in the workforce environment that will also gain momentum.

2013 & 2015 Global Information Security Workforce Study Repondents  
For Leaders, Finding Qualified Personnel is a Rising Contributor to the Workforce Shortage



Leslie Burns, director of Information Security Operations at Target, provided additional perspective on finding qualified personnel that could help in alleviating this workforce shortage: broaden search beyond technical security skills.



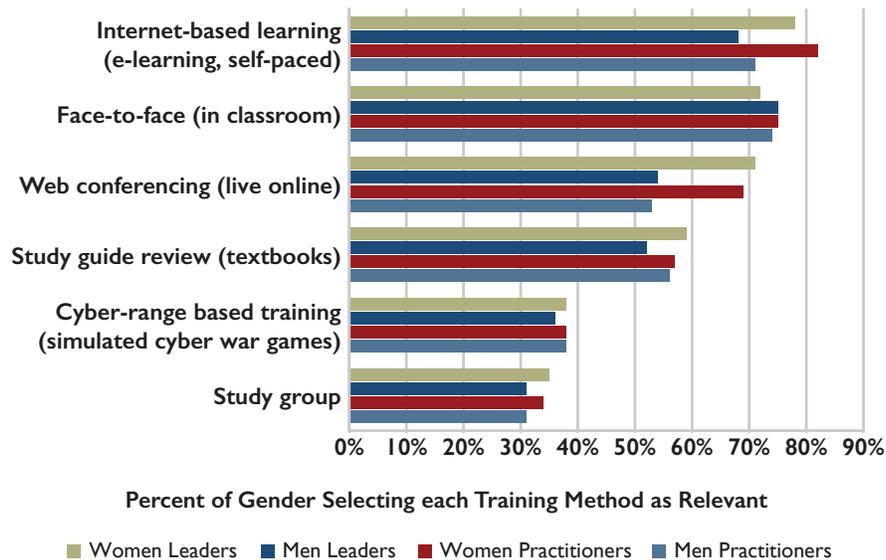
**Leslie Burns stated,** “Today’s threat, compliance, and risk landscapes are significantly more complex, compared to the past. Therefore, skillsets needed in an information security organization have broadened. There will always be roles that require deep technical expertise. However, now there is also a growing demand for roles that require skills like business acumen, problem solving, risk management, and critical thinking.”

“When hiring for this growing demand,” **Burns recommends,** “look for someone who knows the business, has a strong base in technology, and can lead effective change. Some experiences traditionally outside of information security can translate well and be applied to this space.”



In our last piece of analysis, we repeat an observation made two years ago: women are more diverse in their views on training methods. Similar to the need to diversify incentives to retain InfoSec professionals, offering increased accessibility and wider diversity of InfoSec training may also prove to be increasingly valuable in retention and in elevating InfoSec professionals’ readiness to succeed in new roles.

2015 Global Information Security Workforce Study Repondents  
 Women Expressed Greater Interest in Leveraging the Internet for InfoSec Training than Men



## FROST & SULLIVAN

### THE LAST WORD

While women counted as a percent of the InfoSec workforce has been stagnantly at 10%, their positioning in this profession is far from stagnant. In fact, our analysis of the data from the past two (ISC)<sup>2</sup> information security workforce surveys shows that women are quickly converging on men in terms of academic focus, computer science and engineering, and, as a gender, have a higher concentration of advanced degrees.

Academic achievement, however, is just one side of the equation. Another side is where women in InfoSec are having their most material impact and that is in governance, risk, and compliance. According to the 2015 survey, one out of five women identified GRC as their primary functional responsibility. Comparative, one out of eight men hold similar roles.

This data point is important as the GRC role is reflective of where the InfoSec profession is evolving: increasingly focused on business risk management. Both genders signal agreement on this point as both women and men in leadership positions indicated that risk assessment and management, GRC, and incident investigation and response are the skills they most need to build over the next three years. Additionally, both genders indicated that a greater share of them will be in GRC roles in the future.

A common understanding on where the InfoSec profession must and will change is also just part of the equation. Another part is how. Women, more so than men, are looking beyond the current state of double-digit churn in the workforce (i.e., changing employers) and a workforce that is predominately in their middle to late stages of their working careers.

Similar to men, women recognize the strong influence of monetary incentives in job retention, but women also believe that money alone will be insufficient. Non-monetary incentives, such as flexible working arrangements, must be part of an effective compensation package to attract and retain personnel. Also, as continuous training is essential in the evolving InfoSec discipline, women have also raised the banner that training methods cannot be unidimensional. Training must take many forms—traditional and online—to accommodate a diverse, multi-generational workforce.

In the end, the InfoSec profession wants and needs to be defined by more than technical and operational expertise. This profession should be recognized for coupling its practical expertise with an acute level of business acumen in serving their organizations in reaching complex strategic and tactical business objectives. Women, in our assessment, have the foundation to push this coupling of practical expertise and business acumen into the new standard of the InfoSec profession.

Additionally, organizations must take direct actions to increase the pool of women candidates for a career in InfoSec and improve retention. Actions that organizations can take include supporting cybersecurity education in primary schools, offering internships, pairing new InfoSec hires with mentors, and, as the survey described, adapting compensation plans and training to better align with the flexible working arrangements and diverse training options women expressed as important in retaining and engaging InfoSec professionals. The workforce shortage in InfoSec and women's low gender proportion in this profession will be slow to change until there is concerted effort to make InfoSec more attractive and rewarding to women.

#### **Michael P. Suby**

Stratecast VP of Research  
Frost & Sullivan  
mike.suby@frost.com

## WOMEN IN SECURITY RESEARCH REVIEW PANEL

**Angie Messer**

Executive Vice President  
Booz Allen Hamilton

**Gudeep Kaur**

Chief Security Architect  
AIG

**Julie Talbot-Hubbard**

Associate Vice President for IT Engineering, Infrastructure & Operations  
Nationwide

**Karen Kabel**

Operational Support and Security Technology Solutions Manager  
Great-West Life Assurance Company

**Alice Fakir**

Executive Director  
Morgan Stanley

**Andrew Smallwood**

Lead Associate, Strategic Innovation Group  
Booz Allen Hamilton

**Renee Hodder**

IT Risk Management Consultant  
Nationwide

**Leslie Burns**

Director of Information Security Operations  
Target

## ABOUT (ISC)<sup>2</sup>®

Formed in 1989, (ISC)<sup>2</sup> is the largest not-for-profit membership body of certified cyber, information, software and infrastructure security professionals worldwide, with nearly 110,000 members in more than 160 countries. Globally recognized as the Gold Standard, (ISC)<sup>2</sup> issues the Certified Authorization Professional (CAP®), Certified Cyber Forensics Professional (CCFP®), Certified Cloud Security Professional (CCSPSM), Certified Information Systems Security Professional (CISSP®) and related concentrations, Certified Secure Software Lifecycle Professional (CSSLP®), HealthCare Information Security and Privacy Practitioner (HCISPP®) and Systems Security Certified Practitioner (SSCP®) credentials to qualifying candidates. (ISC)<sup>2</sup>'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)<sup>2</sup> also offers education programs and services based on its CBK®, a compendium of information and software security topics. More information is available at [www.isc2.org](http://www.isc2.org).

© 2015, (ISC)<sup>2</sup> Inc., (ISC)<sup>2</sup>, CAP, CCFP, CISSP, CSSLP, HCISPP, SSCP and CBK are registered marks, and CCSP is a service mark, of (ISC)<sup>2</sup>, Inc.

## ABOUT THE (ISC)<sup>2</sup>® FOUNDATION

The (ISC)<sup>2</sup> 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 through its programs and the efforts of its members. Through the (ISC)<sup>2</sup> Foundation, (ISC)<sup>2</sup>'s global membership of nearly 110,000 certified cyber, information, software and infrastructure security professionals seek to ensure that children everywhere have a positive, productive, and safe experience online, to spur the development of the next generation of cybersecurity professionals, and to illuminate major issues facing the industry now and in the future. For more information, please visit [www.isc2cares.org](http://www.isc2cares.org).

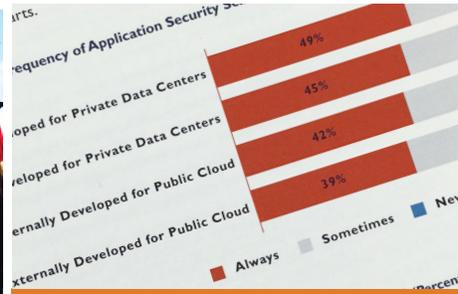
## ABOUT BOOZ ALLEN HAMILTON

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](http://www.boozallen.com). (NYSE: BAH)

Inspiring a safe and secure cyber world through our three initiatives.



Scholarships



Research



Education & Awareness

Empowering the  
**NEXT GENERATION**  
of cybersecurity workers.

Empowering  
**PROFESSIONALS**  
with cutting edge research.

Empowering the  
**PUBLIC**  
with educational resources to secure their online life.

For more information on how you can  
**volunteer, donate, or advocate** please visit:

[isc2cares.org](http://isc2cares.org)

Auckland  
Bahrain  
Bangkok  
Beijing  
Bengaluru  
Buenos Aires  
Cape Town  
Chennai  
Dammam  
Delhi  
Detroit  
Dubai

Frankfurt  
Herzliya  
Houston  
Irvine  
Iskander Malaysia/Johor Bahru  
Istanbul  
Jakarta  
Kolkata  
Kotte Colombo  
Kuala Lumpur  
London  
Manhattan

Miami  
Milan  
Moscow  
Mountain View  
Mumbai  
Oxford  
Paris  
Pune  
Rockville Centre  
San Antonio  
São Paulo  
Seoul

Shanghai  
Shenzhen  
Singapore  
Sydney  
Taipei  
Tokyo  
Toronto  
Valbonne  
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 SW1W 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