FROST & SULLIVAN

Agents of Change: Women in the Information Security Profession

The (ISC)² Global Information Security Workforce Subreport

A whitepaper derived from the 2013 (ISC)² Global Information Security Workforce Study, a Frost & Sullivan market study, in partnership with:

(ISC)²®

Symantec™

contents

INTRODUCTION

The information security discipline is not evolving fast enough. Most notable, women represent just 11% of this profession. Placed in the context of women in the general workforce and women in professional and managerial roles—where women are at near parity with men in both of these measurements in developed countries—this 11% is alarming.

Furthermore, this low percent of women in the information security profession has been stagnant despite double-digit annual increases in this profession. In 2012 alone, the global information security workforce grew by 306,000 and is on pace to increase by another 332,000 in 2013. Yet, these increases have done little to address persistent personnel shortages. Essentially, more information security professionals are needed, but the profession as a whole has been slow in tapping into the pool of talent represented by women.

Also, the information security discipline must transform in how it is practiced. Despite the overall growth in information security professionals and corresponding increases in expenditures on security technologies, the frequency and severity of data breaches, network compromises, and regulatory non-compliance has become a boardroom concern. The status quo is showing its weaknesses.

Women as agents of change in transforming information security is the topic of this report from (ISC)²® and Symantec, using data collected in a late-2012 Frost & Sullivan survey of information security professionals commissioned by (ISC)².

WHY INFORMATION SECURITY DISCIPLINE MUST TRANSFORM

The information security discipline must transform and also address its perpetual shortage in information security professionals. Past transformational approaches, while well-meaning, have only produced incremental and reactionary outcomes and are not keeping pace with the many exogenous factors that are driving demand for more security and risk management, and security professionals.

These pace-setting factors are well-known and include:

- Evolution in threats and threat vectors such as advanced persistent threats, distributed denial of service attacks, and application-layer software compromises
- Introduction and adoption of new technologies such as cloud-delivered services, bring your own device (BYOD), bring your own application, and big data and analytics
- Formation of new business-to-business (B2B) and business-to-consumer (B2C) relationships, driven by user device multiplicity, mobility, the Internet of things, and an intensifying competitive global marketplace
- Scope, complexity and, in some cases, conflicting regulatory requirements

This need for game-changing approaches in information security is corroborated by those most responsible (and accountable) for security and risk management strategies—security executives. These two reports, both based on direct input from security executives, call attention to this need:[1]

- *Transforming Information Security – Designing a State-of-the-Art Extended Team*
- *Fighting to Close the Gap – Ernst & Young's 2012 Global Information Security Survey*

Common among these reports is the perspective that internal security teams must change in two attributes: (1) skill set diversification, and (2) partnerships with organizations that have complementary capabilities, both inside and outside their own enterprises. But in order for change of this nature to occur and change with permanence, there must be *agents of change*—individuals that have the mindset and skill set essential to lead transformation. Where might these agents of change be found? These individuals exist but are in the minority in most security organizations—they are women who have chosen the security profession.

This study shows that women are only beginning to scratch the surface of the Information Security field. (ISC)² is well placed to ensure that there are enough skilled workers to meet the demand both male and female.

— Diana-Lynn Contesti, CISSP-ISSAP-ISSMP, CSSLP, SSCP
Information Security Officer, ArcelorMittal Dofasco, Canada; and
Member, Board of Directors, (ISC)²

WOMEN: HOW MUCH IN THE MINORITY?

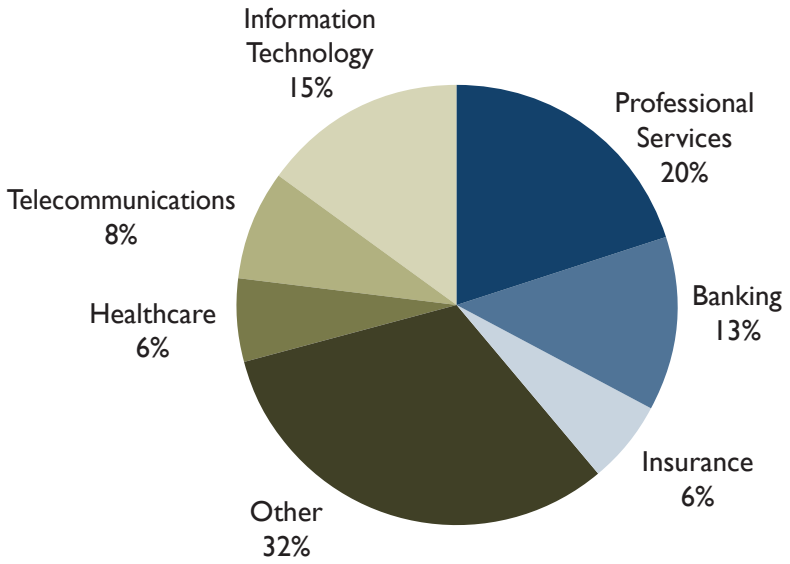
Based on this extensive survey, women represent just 11% of the information security profession globally. Although a notable figure on its own, uncovering the distinctive perspectives of women in security relative to men requires an approach that mitigates biases associated with cultural, regional, industrial, and employer size attributes. This was accomplished by limiting our data analysis to a subset of survey respondents, while still retaining a relevant number of respondents. The subset of data was restricted to these survey respondent parameters:

- Resides in a developed country
- Employed in private industry (versus government of any jurisdiction)
- Employer has 500 or more employees

The resulting survey subset contains 5,814 respondents, which were segmented into two job title classifications:

- **Leaders** (3,466 respondents): Executives (e.g., CEO, CIO, CSO, CISO, etc.), managers, architects, strategists, and strategic advisors
- **Doers** (2,348 respondents): All other job titles, with the most frequently chosen job titles being security analyst (29% of Doers), followed by security and compliance auditors (22%)

Figure 1: Distribution of Security Professionals Across Industries



Combined and in each of the job title classifications, women and men were similarly distributed among industries, with professional services employing the highest percentage of survey subset respondents (20%).

There were a few notable gender differences in job title distribution. In the Leaders classification, a higher proportion of women were in consultant and advisor job titles than men, whereas men had a higher proportion in architect job titles. In Doers, 38% of the women selected security analyst as their job title versus 27% of men. Conversely, higher proportions of men have security engineer and network administor job titles than women.

Figure 2: Job Title Distribution – Leaders

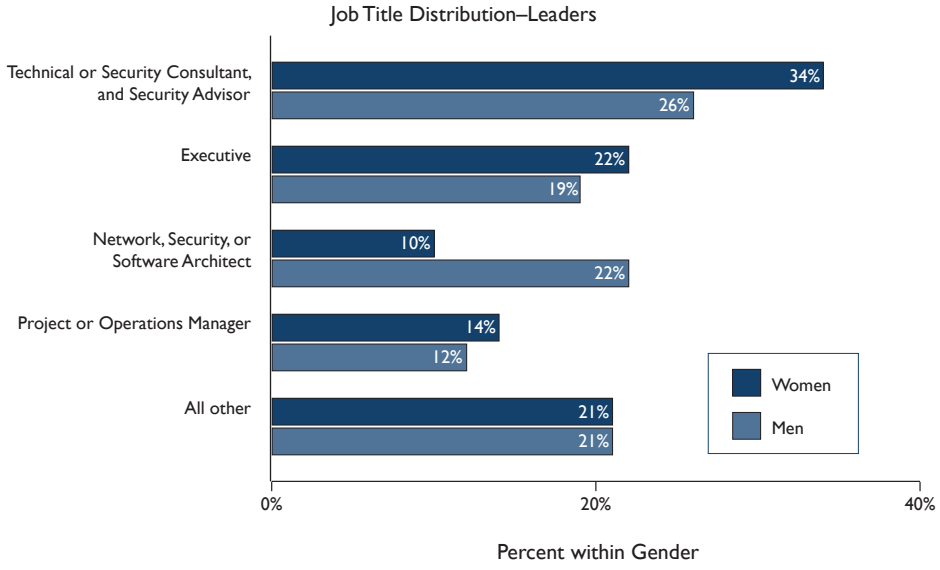
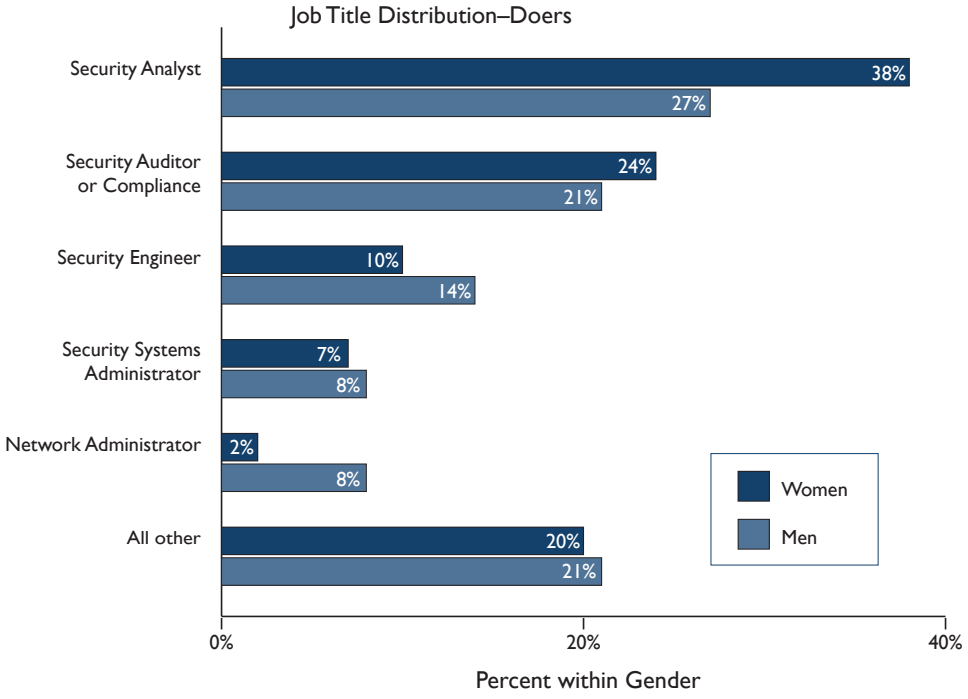


Figure 3: Job Title Distribution – Doers



Within the two job title classifications, average job tenure, median and average annual salary, and academic attainment showed marginal differences between women and men.

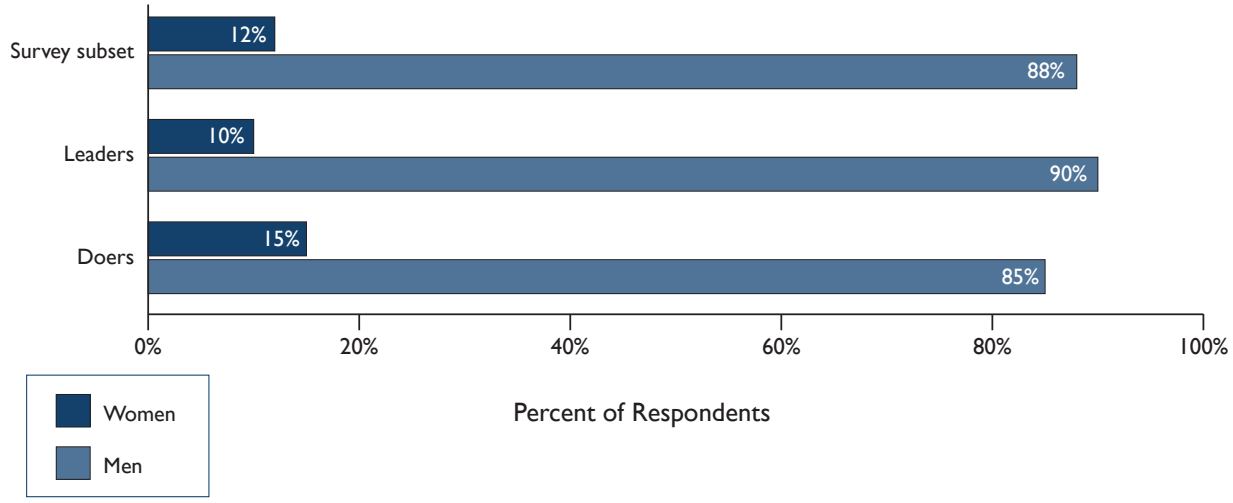
Figure 4: Tenure, Salary, and Academic Achievement Comparison

	Leaders		Doers	
	Women	**Men**	**Women**	**Men**
Average number of years in security profession	13.5	13.6	12.1	12.2
Median annual salary *(salary selections in the survey were presented in $10,000 increments; e.g., $90,000 - $99,999)*	$105,000	$105,00	$85,000	$95,000
Average annual salary	$109,800	$111,100	$91,000	$93,500
Percent with bachelor, masters, or a doctorate degree	91%	89%	91%	85%

In comparison to representative labor statistics—women in 2012 accounted for 46.9% of the United States total labor force (45.6% in the European Union) and 51.5% of United States management, professional, and related positions—it is clearly evident that women, at just 11% of the information security profession, are greatly under-represented.[2]

Although not a surprising directional result, given the historical male dominance in the information security profession, this low representation by women raises questions: Is this profession not as appealing to women as other professions? And, is this profession missing a beneficial opportunity to employ and promote more women?

Figure 5: Gender Distribution in Information Security



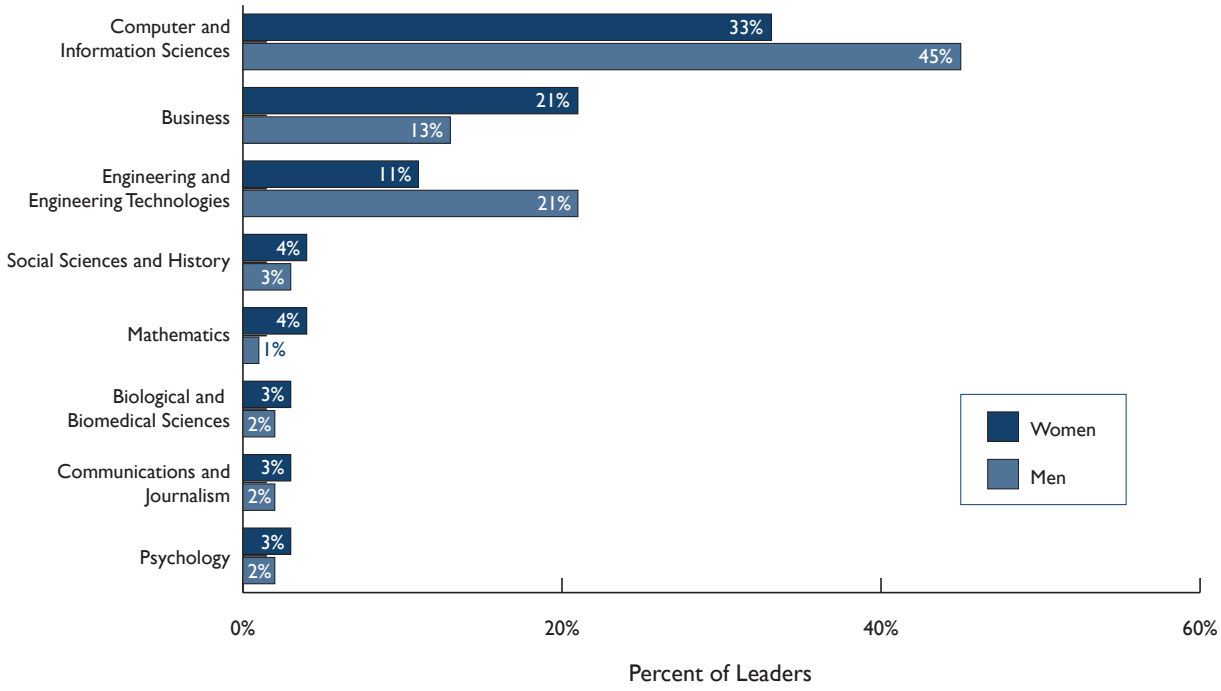
> It is evident today that women in the information security profession are greatly underrepresented. We need to recognize the strengths that women bring, such as their diverse academic backgrounds and differentiated skill sets, and make training more widely accessible to encourage more women to pursue this career path.
>
> — Julie Talbot-Hubbard,
> Vice President and Chief Security Officer, Symantec

DIFFERENTIATED SKILL SET

In looking at the skill sets and backgrounds of women, we examined two questions: what are the skill sets and backgrounds of proven successful information security professionals, and what are the skill sets and backgrounds being sought by security organizations hiring new employees? For this, we concentrated on respondents in the Leaders category due to their higher career advancement (a proxy for success) and their involvement in hiring decisions.

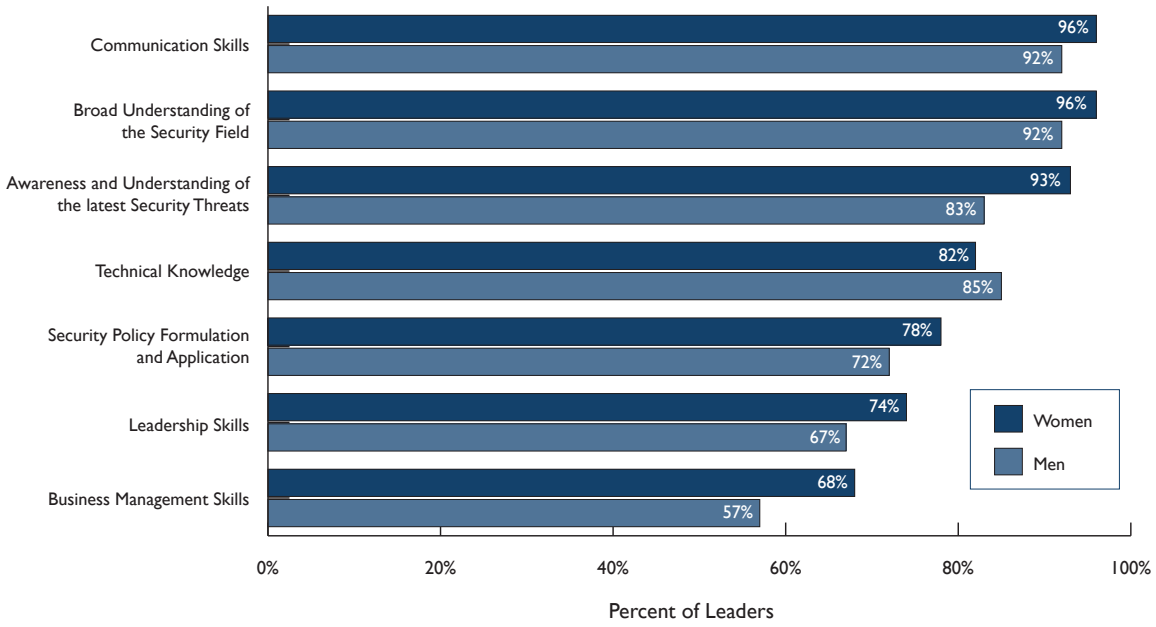
As shown in this chart, women in security, as a group, have a more diverse academic background than men, and a collective background with slightly greater emphasis on social sciences and significantly less emphasis on the majors traditionally associated with the security workforce (i.e., computer and information sciences, and engineering). On this latter point, undergraduate major selection is influenced by several, changeable factors. Those factors include: market conditions (i.e., future job prospects), erosion in gender-bias career stereotypes, and the career guidance and mentoring high school and college students receive. Supporting this point is the parity in the percent of women (47%) and men (48%) in the Doer classification that had computer or information sciences as an undergraduate major. As an indicator of more women choosing and graduating with this major, this bodes well for more women entering the security career when a computer or information sciences major is a primary job candidate filter.

Figure 6: Undergraduate Major-Leaders



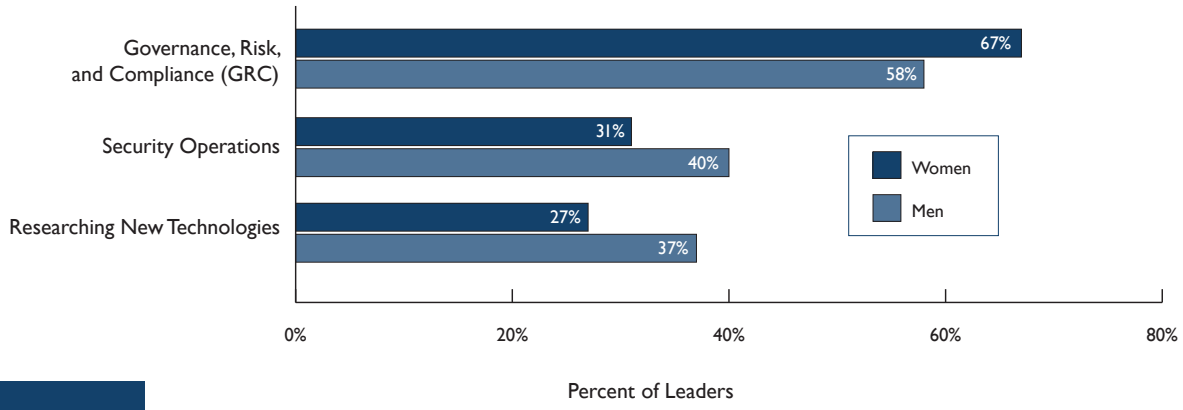
Similar diversity is evident in women's perspectives on the skill attributes associated with a successful information security professional versus men's perspectives. While graphically the differences seem slight, these differences are nevertheless statistically significant with the exception of technical knowledge—the sole category selected by a smaller percentage of women as very important or important. Our interpretation is that technical knowledge is not becoming less important; rather, other skills that cut across disciplines are growing in importance with both genders, but more so with women.

Figure 7: Skill Attributes of a Successful Information Security Professional (Very Important and Important)



This interpretation aligns with the data showing the differences in how women and men security leaders spend their time. As shown in the next chart, women leaders are engaged to a greater extent in governance, risk, and compliance (GRC) than their male counterparts and less in operational duties. Advancing GRC goals requires more coordination across organizational boundaries than in highly exclusive security roles (e.g., researching new security technologies), a logical reflection of the data showing women's relatively higher rating of importance assigned to skills that contribute to cross-organizational collaboration. Furthermore, as organizations continue on their journey to align security strategy with business strategy, a point emphasized in the aforementioned Ernst & Young study, the discipline of GRC and demand for skills that support GRC will intensify.

Figure 8: Spending Significant Amounts of Time



TAKES A COMMUNITY APPROACH

Security and risk management should be an all-inclusive responsibility, not just resting on the shoulders of the select few in the information security profession. This sentiment is supported by the survey—nearly all of the areas where survey respondents indicated growing demand for training and education reach into the rank-and-file. The few that are purely in the security professional's domain are logically so; for example, forensics, and to a lesser extent because the responsibilities would be shared with software developers and system administrators, application and system development security.

Also evident in the survey is that women leaders are the strongest proponents of security and risk management education and training. In this chart, not only do they exceed male leaders' demands for training and education in security and risk management, they also exceed the security Doers (there were not statistically significant differences between women and men Doers in their views on this topic).

Figure 9: Areas of Growing Demand for Education and Training

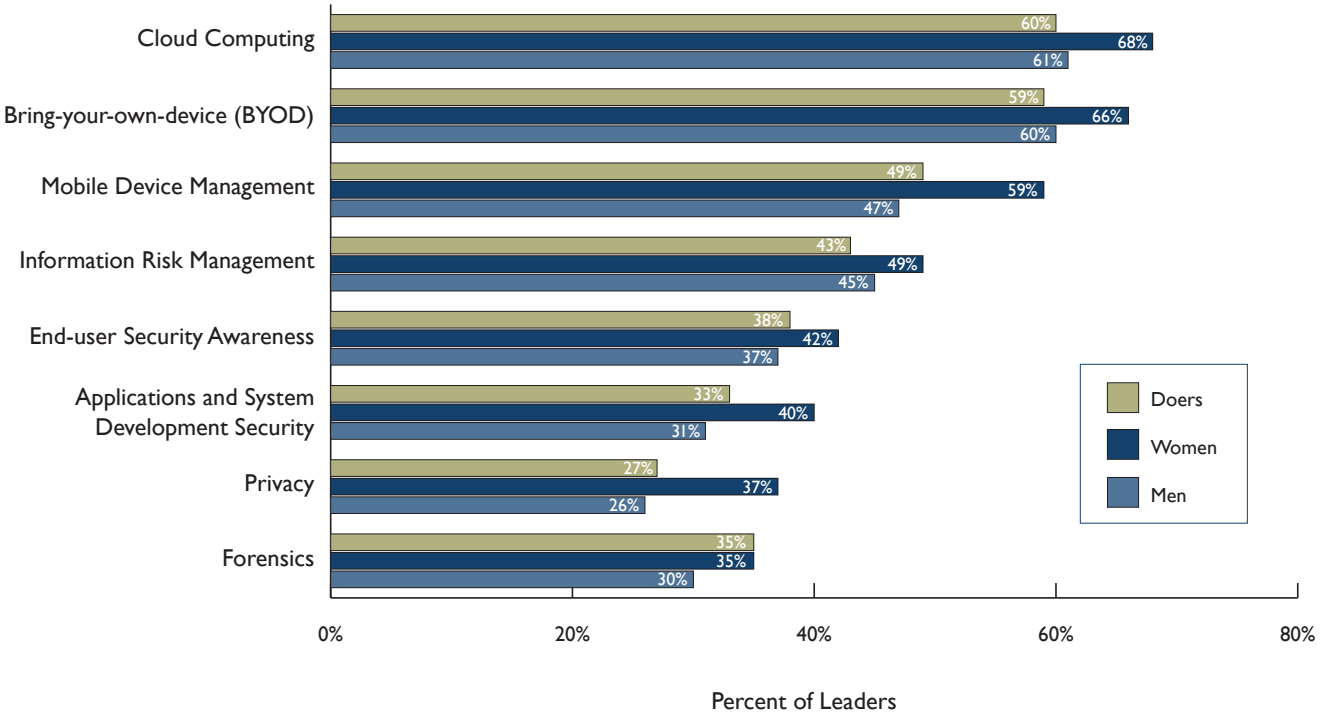
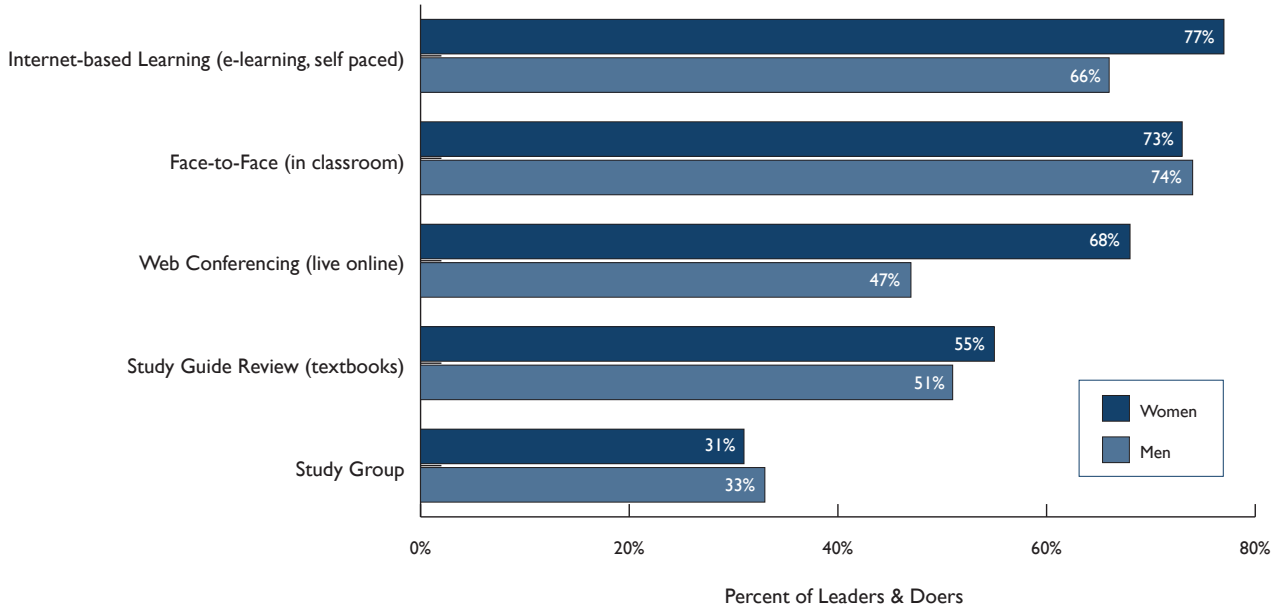


Figure 10: Relevance of Training and Education Method



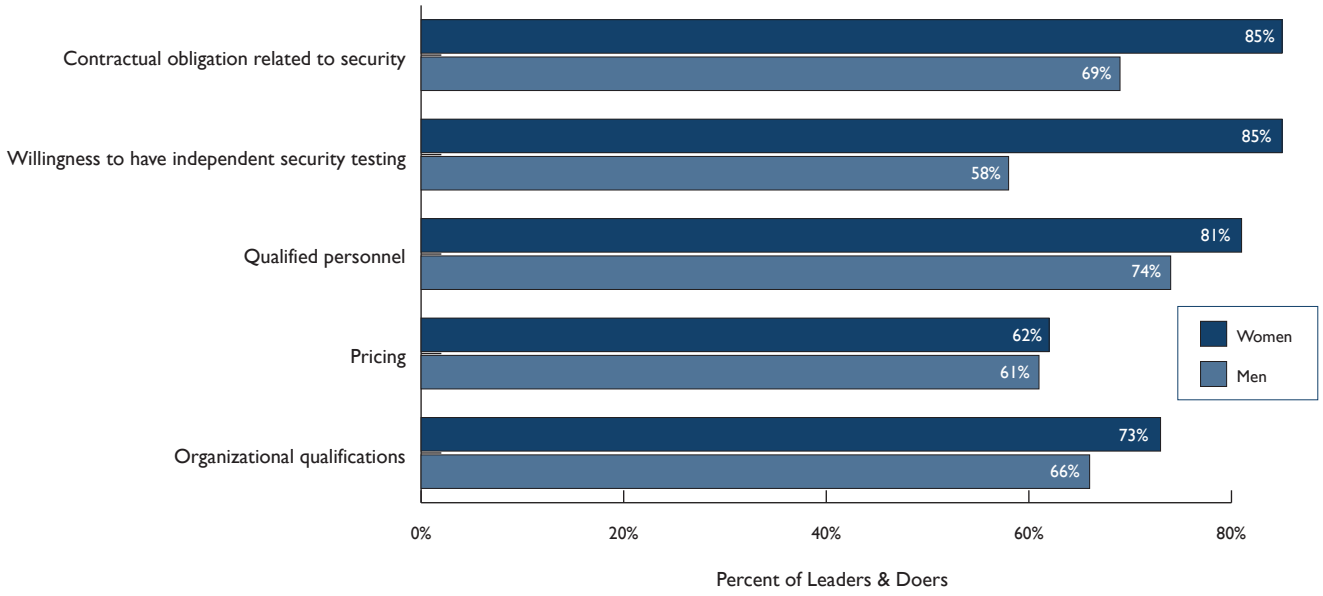
A related topic to demand for security training and education is how training and education are delivered. Here, too, the survey uncovered significant differences between the genders. Women, both Leaders and Doers, are stronger advocates of Web- or Internet-based training and education methods than men. Considering the previously stated precept that security and risk management is a shared responsibility, training and education must be widely accessible and, because budgets are never unlimited, affordable (e.g., a declining cost per training session as the number of sessions or participants increase). Relative to old-school methods, online is the logical choice and women are ahead of men in their advocacy of online training and education.

In promoting a community approach to security and risk management, partnerships with third parties are inevitable. Substantiating this inevitability is the perspective of security executives in their forecasted future use of managed and professional security services—nearly one-third of security executives in our survey are predicting a year-over-year spending increase. Yet, with expanding use of third parties, how will client organizations ensure that they receive the quality, quantity, and timeliness they paid for? Perhaps telling is how women leaders are answering this question—"make it formal and verifiable." This position, much more strongly voiced by women than men, is demonstrated in women security leaders' answers to our survey question on selecting a

"Meeting the challenges of cyber security requires a diverse and engaged community; achieving gender balance in our profession is an obvious and vital place to start addressing this need. We must ensure that diversity-focused information security professional programs drive true change in our profession to equip the workforce of tomorrow, and that future generations of all genders find a welcoming and engaged community of information security colleagues.

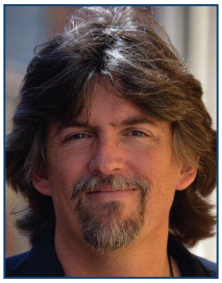
— Dan Houser, Sr., CISSP-ISSAP-ISSMP, CSSLP, SSCP
Security & Identity Architect, Cardinal Health Systems, Columbus, OH, USA;
and Member, Board of Directors, (ISC)²"

Figure 11: Importance in Selecting a Partner for Software Application Development ***(Top and High Importance)***



partner for software application development. The differences between women and men security leaders in contractual obligations and independent security testing are, as shown, very significant.

Also noteworthy in the context of software application development is the previously displayed higher emphasis by women over men on education and training in application and system development. As software vulnerabilities are a topmost concern for information security executives (72% of information security executives in the global survey selected software vulnerabilities as a top or high concern), women's relatively higher focus on internal training and education and the pragmatic aspects of partner selection demonstrates women's attention to deep-rooted issues of security risk and in devising plans to mitigate risk.



"The Information Security industry needs to lead the charge in shaking off the archaic image of being a "guys only" profession – an image which seems largely responsible for discouraging young women from choosing the academic programs that lead to careers in InfoSec, or IT in general which suffers a similar disparity. Initiatives such as the (ISC)² Foundation's Women in Security are key to addressing this issue at a grass-roots level, and are critical to instigating, and maintaining, the change that is so badly needed."

— Richard Lane, CISSP-ISSMP
Head of Information Security for an International Organization and Lead Volunteer, Safe and Secure Online Switzerland

The Last Word

The practice of information security is transforming to a more comprehensive, risk-based, business orientation. From a positive perspective, security professionals are in an ideal position to lead rather than follow in this transformation. They, more than personnel in other departments, have the baseline covered: that is, understanding of security threats, and knowledge and use of mitigating techniques and technologies. But effective transformation will take more than functional understanding and operational expertise; an advocacy of continuous education and community-building, as well as ability to balance the subtleties of risk and business objectives will be required.

From our survey of information security professionals, we identified areas where women in the security profession, collectively, show distinctive perspectives relative to their male counterparts. Many of these distinctive perspectives align with the traits needed to transform the direction, operating practices, and priorities of security organizations. As commercial and public enterprises start their transformational journey or are seeking to accelerate, they should take into account the personnel traits necessary to ensure an effective transformation. It may be that this set of traits is within their existing security organizations but outside the "average."

Enterprises should also consider the steps that they can make to encourage more women to pursue the information security profession and, for those in the profession, to stay. Foremost among those steps is for the male leadership in and out of the information security field to recognize the concrete and complementary value that women bring to information security. Also, in their recruiting and hiring decisions, greater emphasis should be placed on building a more diverse information security team. Technical skills, while still important, must be increasingly supplemented with the multi-disciplinary skills and perspective necessary to make subtle but impactful risk management decisions.

Michael P. Suby
VP of Research
Stratecast | Frost & Sullivan
msuby@stratecast.com

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

(ISC)² is the largest not-for-profit membership body of certified information security professionals worldwide, with nearly 90,000 members in more than 135 countries. (ISC)²'s certifications are among the first information technology credentials to meet the stringent requirements of ISO/IEC Standard 17024, a global benchmark for assessing and certifying personnel. (ISC)² also offers education programs and services based on its CBK®, a compendium of information security topics. The (ISC)² Foundation is the charitable trust of (ISC)², aiming to make the cyber world a safer place for everyone with community education, scholarships and industry research like the (ISC)² Global Information Security Workforce Study. More information is available at www.isc2.org and www.isc2cares.org.

ABOUT SYMANTEC

Symantec protects the world's information, and is a global leader in security, backup and availability solutions. Our innovative products and services protect people and information in any environment—from the smallest mobile device, to the enterprise data center, to cloud-based systems. Our world-renowned expertise in protecting data, identities and interactions gives our customers confidence in a connected world. More information is available at www.symantec.com or by connecting with Symantec at: go.symantec.com/socialmedia.

ENDNOTES

1. These two reports, respectively, are accessible at: http://www.emc.com/collateral/white-papers/h12227-rsa-designing-state-of-the-art-extended-team.pdf and http://www.ey.com/Publication/vwLUAssets/Fighting_to_close_the_gap:_2012_Global_Information_Security_Survey/$FILE/2012_Global_Information_Security_Survey___Fighting_to_close_the_gap.pdf.

2. US Bureau of Labor Statistics and http://epp.eurostat.cc.europa.eu/statistics. For context, 57% of the survey subset respondents reside in the United States, 7% in Canada, and 26% in Europe.

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

Silicon Valley
331 E. Evelyn Ave. Suite 100
Mountain View, CA 94041
Tel 650.475.4500
Fax 650.475.1570

San Antonio
7550 West Interstate 10,
Suite 400,
San Antonio, Texas 78229
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