Women in Cybersecurity

Submitted in partial fulfillment of the requirements for the degree of Master in Public Policy

Prepared by
Katharine D’Hondt
Master in Public Policy Candidate
May 2016

Client: Megan Garcia, New America
PAE Advisor: James Waldo
PAC Seminar Leader: Phil Hanser

March 29, 2016

This PAE reflects the views of the author and should not be viewed as representing the views of the PAE's external client, nor those of Harvard University or any of its faculty.
Acknowledgements

I am so grateful to my client team at New America. Megan Garcia, Elizabeth Weingarten, Brooke Hunter, and Courtney Schuster have been incredibly welcoming, thoughtful, and encouraging throughout this process. I am thankful to have had the chance to meet Megan, Elizabeth, and Brooke in person on two occasions, both of which were times when I had the chance to see New America’s work in action. I will continue to strive for their passion, drive, and creativity in my professional life.

I am also thankful to my advisor, Professor Jim Waldo, for his feedback, candor, humor, and passion about this problem and how to solve it. Jim’s willingness to connect me with women in the field added a depth to this project that would not exist otherwise. I met Jim through his cybersecurity course at the Kennedy School, a course that continues to shape my professional interests and trajectory.

I am especially grateful to all of the cybersecurity professionals who took the time to speak with me about the problem of women’s underrepresentation in the field. These open and constructive conversations shaped the direction of this research and formed my understanding of how to approach this project.

I would also like to thank the Harvard Kennedy School’s Women and Public Policy Program and its Lara Warner Scholars Program. Without Ms. Warner’s generous funding and support, I would not have been able to attend New America’s November 2015 convening of women in cybersecurity in San Francisco or New America’s cybersecurity conference in March 2016.

I am thankful for the support of Harvard National Security Fellow Steve Anderson. Steve edited multiple versions of my PAE and connected me with colleagues whose insights heavily informed the final version of this report.

The work of the Harvard Women in Computer Science group, particularly Ramya Rangan and Jn Fang, was integral to this project. Without their brilliant survey design, survey deployment, and collaboration, the data analysis section of this report would not have been possible.

It was truly an honor to join the board of the Harvard National Center for Women in Information Technology (NCWIT) project. This experience showed me the challenges and success factors in addressing this problem at a smaller scale, specifically at the level of the Harvard University computer science department.

My PAC seminar leader, Phil Hanser, was tremendously helpful in editing this piece, as well as guiding my thinking towards resources related to the STEM workforce.

Finally, I cannot thank my family enough for their endless support throughout my time at the Kennedy School. Specifically, I would like to thank my parents who taught me the importance of education and hard work.
# Table of Contents

Acknowledgements ........................................................................................................... 1  

Executive Summary .......................................................................................................... 3  
  Findings ......................................................................................................................... 4  
  Recommendations ......................................................................................................... 5  

Introduction ..................................................................................................................... 7  

Methodology ..................................................................................................................... 10  

Literature Review .............................................................................................................. 11  
  Childhood ....................................................................................................................... 11  
  Post-Secondary Education ............................................................................................. 12  
  Workforce Entry ........................................................................................................... 14  

Case Studies from Other Industries .................................................................................. 16  
  Medicine: Radiology ...................................................................................................... 16  
  Law .................................................................................................................................. 17  

Findings from Expert Interviews ....................................................................................... 20  
  Successes ....................................................................................................................... 20  
    Mentorship .................................................................................................................. 20  
    Scholarships ............................................................................................................... 21  
    Prominence of Women in Culture, Leadership, and Branding ..................................... 21  
  Barriers .......................................................................................................................... 23  
    Militaristic/Male-Gendered Culture and Stereotypes ................................................... 23  
    Recruitment ............................................................................................................... 25  
    Bias in the Hiring Process and Workplace .................................................................... 25  
    Branding ..................................................................................................................... 26  

Harvard Women in Computer Science Data Analysis ...................................................... 28  
  Findings ......................................................................................................................... 28  
  Analysis ......................................................................................................................... 30  
    Perceptions of the Gender Gap in Computer Science .................................................. 30  
    Gender and Computer Science Experience ................................................................ 30  
    Self-Assessment of Skills by Gender ........................................................................ 30  

Policy Criteria and Analysis .............................................................................................. 31  

Recommendations and Implementation ........................................................................... 32  
  Assessment .................................................................................................................... 33  
  Branding ......................................................................................................................... 36  
    Language .................................................................................................................... 36  
    LinkedIn ..................................................................................................................... 37  
    Scholarships and Continuing Education ................................................................. 37  
  Culture Change ............................................................................................................ 38  
  Mentorship .................................................................................................................... 40  

Conclusion ......................................................................................................................... 41  

Appendices ......................................................................................................................... 42
Executive Summary

The underrepresentation of women in cybersecurity is a critical national security and business problem. While making the case for gender parity in the field is significant from a social justice standpoint, research shows it is also imperative to consider it through economic and national security lenses. The U.S. Department of State, Target, Visa, MasterCard, the U.S. Office of Personnel Management, and others have all been victims of serious cyber-attacks, including distributed denial of service attacks, information theft, and more, in the last five years. (Risen, 2015) If an inadequate supply of cybersecurity professionals leaves these supposedly secure entities unable to protect themselves against cybersecurity threats, this danger will worsen as the shortage of cybersecurity professionals grows. The current shortage is projected to reach 1.5 million unfilled positions by 2020. (Suby, 2015) One cause of this problem is a lack of diversity in the field. In particular, women are dramatically underrepresented. Without a plan to grow the cybersecurity workforce by attracting more women to the field, prominent businesses and government agencies will become increasingly vulnerable due to cyber-attacks just when attacks by rogue states, terrorists, and criminals are projected to increase. The nation and its companies are at an acute risk of losing money, time, privacy, and credibility without an adequate workforce to address cybersecurity problems.

New America's Women in Cybersecurity Project requested this research given its alignment with its mission to bring together cybersecurity companies, government, and big thinkers to promote methods to bring women into the cybersecurity field. Launched in 2015, the Women in Cybersecurity Project started as a joint initiative between New America’s Better Life Lab and Cybersecurity Initiative. The team recently established fundamental pillars of its work to include research, communications, and building a toolkit for New America's partners. Led by Megan Garcia, the team provided the objectives of this research project:

- Research what companies, universities and non-profit groups are doing already about underrepresentation of women in the cybersecurity field.
• Develop case studies of industries in which women or other minorities have been underrepresented, and in which representation improved. What worked? What did not? What internal and external factors played a role?
• Use findings from New America’s convening of women in cybersecurity in November 2015 to develop recommendations about how the New America Women in Cybersecurity project should proceed.

This report will inform New America’s toolkit and the strategy as it makes the economic and business case for increasing the representation of women in cybersecurity to a wide network of corporate partners and the general public.

Findings
Expert interviews, quantitative analysis of student survey data, and academic research informed this analysis and subsequent recommendations. There are several reasons why women drop off at various points when developing a career in cybersecurity. The first two findings present as “shrinking the talent pipeline” problems, while the final finding presents as a “keeping them” problem. This report not only identifies the reasons for difficulty in recruiting and retaining women in cybersecurity but also outlines potential solutions to these barriers.

• **Militaristic/gendered culture and language alienate women looking to enter the field:** Given cybersecurity’s roots in high-security military operations, it is no wonder that the use of heavy military language and a male-dominated culture persists. Women have a hard time imagining themselves in this type of culture. Therefore, fewer pursue careers in it. The White House, among other organizations, has made a push to shift terminology away from cybersecurity towards information security, a term which may present a more holistic (and inclusive) picture of the field.

• **The cultural biases of influencers and decision makers inhibit women’s entry in the field:** Studies show that in women’s formative experiences, teachers, parents, and mentors may consciously or unconsciously steer them away from fields seen as more masculine. In doing so, they unintentionally decrease the future talent-pool for these
fields. Later, gender-based biases of predominantly male hiring managers often confront women looking to enter the field. For example, at New America’s November convening of industry leaders, one participant noted that identical pieces of code received lower scores when attached to female (as opposed to male) names during the hiring process.

- **Realities and perceptions of work/life balance drive women away:** For women with family caregiving expectations, the pressure of long or irregular hours make it difficult to stay in the field in the long run. To keep up with the fast pace of cybersecurity, professionals face long hours on top of rigorous continuing education to obtain necessary certifications and technological skills.

**Recommendations**

To address the findings above, New America requested recommendations for its business partners to promote inclusion and drive an increase in the number of women entering and staying in the cybersecurity workforce. These recommendations include:

- **Assess the organization’s current practices:** Organizations should qualitatively and quantitatively assess the current efficacy of workplace policies to increase the recruitment and retention of women in their cybersecurity operations. Evaluation is an underlying, critical component of all of the following recommendations.

- **Create inclusive branding:** Information security organizations and contractors often design male-oriented websites and promotional materials that are not only unattractive but sometimes exclusionary to women. Female interviewees mentioned alcohol-intensive branding and ‘boys’ club’ messaging as prominent features of many information security recruiting pages.

- **Fund the talent:** The industry should establish scholarships and continuing education programs tied to current or future employment to serve as a key success factor in getting and keeping women in the field. The longevity and success of these programs relies on showing the return on investment.

- **Reduce the use of militaristic language:** Studies show women prefer occupations allowing them to create results for humans, as opposed to networks. Using less
militaristic and impersonal language will draw more women to the field. Language is pervasive. This means that organization’s website, job announcements, interview language, and office culture should reflect this shift in terminology.

- **Identify and control for hiring biases:** This report puts forth implementable tools to check for common biases in hiring managers. For example, a blind application review can prevent equal technical skill (such as coding) from being scored differently depending on whether a male or female name is attached to it.

- **Mentor women to retain them:** In an overwhelmingly male field, women may find it difficult to navigate everything from salary negotiations to normal day-to-day interactions or social office events. By providing structured opportunities for mentorship, women will have a safe space to discuss these challenges. Mentoring programs, coupled with intensively evaluated leadership programs, “offer great promise.” (Bohnet, 2016)
Introduction

Though women make up 47% of the U.S. labor force (Labor, 2010), they only represent roughly 10% of the cybersecurity field. (Suby, 2015) The U.S. Bureau of Labor Statistics forecasts that employment of information security analysts will grow 18 percent from 2014 to 2024, “much faster than the average for all occupations.” (Bureau of Labor Statistics, 2015) Given the projected increase in demand for these professionals, there are huge risks associated with women’s underrepresentation within business and government when considering the projected need for depth and diversity of talent. With present trends, the government and private sector simply will not have enough cybersecurity workers to create and protect their information and online infrastructure.

President Obama has stressed the vulnerabilities related to cybersecurity in everything from executive orders to his most recent budget proposal. On February 12, 2013, he issued Executive Order 13636, “Improving Critical Infrastructure Cybersecurity,” to establish that “[i]t is the Policy of the United States to enhance the security and resilience of the Nation’s critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties.” (NIST, 2015) Human capital underlies these critical components of infrastructure. People must make decisions impacting network security. Cybersecurity organizations aspire to the National Institute of Standards and Technology’s “Framework for Improving Critical Infrastructure Cybersecurity,” one of the outputs of President Obama’s executive order. However, without a robust workforce as well as a diversity of perspectives in implementing the NIST framework, vulnerabilities will persist.

Since the release of this executive order, businesses and government agencies have been slow to address the dearth of female representation in cybersecurity, despite the opportunities and

Defining Cybersecurity

This report defines cybersecurity and information security as any occupation that “plans [or] carries out security measures to protect an organization’s computer networks and systems. These responsibilities are continually expanding as the number of cyber-attacks increases.” (Bureau of Labor Statistics, 2015)
benefits presented by increased representation. From a product development perspective, the large gap in women’s representation raises concerns about the assembly of gender-diverse teams and the ability to innovate in the rapidly changing cyber landscape. Women’s participation in an otherwise male-dominated group drives up the “predictive power... of a group’s collective intelligence,” due partly to women’s higher scores of social sensitivity measures, which “provide the necessary glue to connect all member’s contributions.” (Bohnet, 2016) From the talent acquisition perspective, cybersecurity professionals are deemed ‘mission-critical’ in government and highly sought after in the private sector. Cyber threats and attacks, such as the Target credit card breach in 2013, constitute huge financial vulnerabilities for businesses. Cyber attacks are also severe problems for government, as illustrated by the recent breach at the U.S. Office of Personnel Management, where the personal information of thousands of government employees was compromised. (Risen, 2015) There is a clear business case for investment in human capital in this industry, both in the private and public sectors.

Why then is 51% of the U.S. population still significantly underrepresented in the cybersecurity field? Academics and professionals point to several reasons for this gender gap. Some commonly cited reasons for women’s hesitance to pursue the field include social and cultural factors related to gender. For example, both toy industry standards and parental biases prompt children to label toys as ‘boy’ or ‘girl’ toys. This shifts girls’ perspective of what is expected from them in terms of academic and personal interests. For example, the computer was heavily marketed as a ‘boy’ toy for several years following its introduction to the market. (NPR, 2014) Others point to the perceived ‘brogrammer’ culture in the cybersecurity field. The term ‘cybersecurity’ itself harkens back to the heavily, militaristic roots of the field. Without a more explicit tie between how networks and systems feed into business operations, women may discard the field without truly understanding what it is about or the opportunity it presents.

Fortunately, research suggests that these social and cultural barriers can be diminished or overcome by effective role models, mentorships, and scholarships. However, the reality is that few organizations execute these programs well. For those that do, the programs have not achieved financially sustainable scalability. This research aims to identify best practices to implement in low-cost, feasible ways.
While much of this research is focused on the transition from post-secondary education to the workforce, it is important to consider retention as an equally severe challenge to approaching gender parity in the workforce. For many women, when a company does not offer policies such as parental leave or flex-time, it forces them into a trade-off between staying in the workforce and completing caregiving responsibilities. Depending on workplace culture, employees may use these policies only to realize real or perceived penalties. As case studies of the medical and legal fields demonstrate, these problems are not unique to the cybersecurity field and are echoed in many sectors where women are underrepresented.

Though cybersecurity is a relatively new field, efforts to correct the challenges outlined above have been incremental and the representation of women in this field as a whole has remained static. This research will focus on women’s perception of the cybersecurity profession for entry-level positions. It will also focus on how companies can adjust their marketing and human capital strategies to attract *all* talent in a more inclusive way. It is crucial to mention that retention in each component of the talent pipeline progression - from secondary school through to mid-career management - feeds into subsequent pipeline problems in the next stage of career development. While the transition from education to the workforce presents many challenges for women in the cybersecurity industry, there is more work to be done in other areas of the talent pipeline.
Methodology

The research employs two main methodologies. The first is a qualitative synthesis of findings from previous academic research along with interviews with experts in the field on prominent barriers to women in cybersecurity at every stage of the school-to-work pipeline. This method also elicits commonly employed solutions and examines best practices from other industries that have shifted towards a more gender-balanced workforce. Prominent takeaways and strategies for success are included based on their anticipated effectiveness in the cybersecurity field.

The second methodology is a quantitative examination of survey data about women’s perceptions of cyber-related careers collected by the Harvard College Women in Computer Science group. Collected in 2015, the current sample size exceeds 700 students and includes both men and women, who are both computer science and non-computer science students at Harvard College. Regression analysis determined if students have statistically significant differences in attitudes towards the interplay of gender and computer science. These findings provide a crucial snapshot of attitudes influencing the pipeline from post-secondary education towards employment. Findings from this survey data are assumed to have some external validity, because they mirror a similar study conducted at Carnegie Mellon University, outlined in the literature review.

The findings from these methodologies inform the prioritization of policy recommendations and next steps based on criteria outlined by New America. As mentioned, New America plans to deploy a toolkit based on these findings for government agencies and business to use to recruit and retain more women in cybersecurity.
Literature Review

As a relatively new field, research about women’s underrepresentation in the cybersecurity field is nascent and therefore limited. However, there is extensive study of women’s underrepresentation in the science, technology, engineering, and math (STEM) fields. To provide a holistic view of the challenges in increasing the representation of women in cybersecurity, this study presents findings from selected literature to reflect women’s progression in the industry from primary education to the workplace. The literature review focuses on common reasons for the drop-off in women’s interest or intent in STEM or cybersecurity-related occupations at each stage. While the studies may not all represent cybersecurity, many parallels can be drawn between STEM fields and cybersecurity due to similar cultural constructs, media messages, and other barriers to entry. Appendix I provides context on the unique development of the cybersecurity field and some crucial insights about how it differs from other STEM fields.

Childhood

For many, the decision to pursue a career in computer science, a feeder field for cybersecurity, solidifies early on due to family factors related to encouragement and exposure. (Wang et al., 2015) Outside of the home, there are many deterents to girls’ interest in STEM, such as a “lack of female STEM character in pop culture, negative stereotypes about girls’ abilities, and negative perceptions about computing as a course of study or career option.” (Wang et al., 2015) However, biases about girls’ abilities held by parents and teachers reinforce these deterring social factors. Such biases are often reflected in a family’s consumer choices: “Families purchase more STEM games or manipulative materials for boys than for girls, and parents of boys believe that their children like science more than parents of girls, more often overestimating their child’s science ability than do parents of girls.” (Wang et al., 2015) While these early influences may seem trivial, they have huge impacts on a child’s perception of what is feminine or masculine, or accessible or inaccessible.

Therefore, it is crucial to examine how socialization and exposure early in the pipeline affect later choices about career and education. These societal factors have an influence not only on prospective female cybersecurity professionals, but also on the people who raise them, and later,
hire them. No series of studies on this topic is more impactful or brilliantly straightforward than those based on the “Draw a Scientist” test, an open-ended projective test designed to investigate children’s perceptions of the scientist. These studies have applications to the underrepresentation of women in cybersecurity due to the similarly technical nature of the work, male dominance in the field, and the ability to replicate the study and findings across time and countries with astounding similarities.

In the last 50 years, when asked to draw a scientist, a vast majority of children, regardless of nationality, will draw “an elderly or middle-aged male in a white coat and glasses who worked in a laboratory, where he performed dangerous experiments.” (Finson, 2002) In a 1981 iteration of this experiment, Chambers reported that only 28 out of the 4,807 elementary school students’ drawings depicted female scientists. This is important because “the stereotypical perception contributes to the frequent misbelief that a scientist must be a genius, enjoy working alone, and have a limited social life. Students who perceive themselves in such a role will be unlikely to pursue a scientific career.” (Finson, 2002) Young women are more likely to pursue a field where they can see others like them. These pervasive stereotypes can limit girls’ sense of what is attainable or acceptable for them academically.

Post-Secondary Education

There are several factors that can influence a woman’s decision to pursue an educational track that feeds into the cybersecurity profession. Studies conducted in the computer science department at Carnegie Mellon University collected information about female students’ attitudes towards one of cybersecurity’s feeder fields, computer science. Carnegie Mellon’s program is significant because it was one of the first to achieve full gender parity among students in the computer science departments. (Blum, 2001)

Carnegie Mellon’s study outlines three key findings, obtained through interviews with students in the program:
1. Women identify a gender gap in computer science experience prior to college, such that male students are coming into the field with more experience. This is not surprising given socialization factors drawn upon in the “Draw a Scientist” research, among other pieces of research.

2. Researchers reported a gap between perceived and actual ability of female students. This carries into a confidence gap seen between men and women in introductory courses. Fortunately, researchers report that the confidence gap narrows as students advance through the major into more difficult courses.

3. Echoing the first finding, previous hacking experience is not cited as a prerequisite for success in computer science. (Blum, 2001)

Different attitudes towards computer science at Carnegie Mellon based on gender (Blum, 2001):

“But I like just what a computer can do. I don't know why it interests me so much...They say kids like to take things apart and see what makes them go and I do that a lot....”
- Male respondent in the Carnegie Mellon study

“What I would really like to do is teach...would like to minor in education and how computers affect education and what is the most efficient way to use them in education.”
- Female respondent in the Carnegie Mellon study

The study also identified different motivations for the study of computer science that fell along gender lines. For men, computer science presented the ultimate toy to tinker with and explore. For women, it was frequently seen as a tool that could be used to achieve a greater, typically socially motivated purpose. Different motivations for entering the major may often reflect in different types of career decisions following graduation.
**Human Centered Design**

“This holistic approach to design takes inspiration from real people, works within market and technological constraints, and considers every product touch-point as an opportunity to surprise, delight and deliver benefits to users.” (Thomsen, 2015)

Given the underrepresentation of women in the computer science field and the motivations outlined for women who are in the major, there could be a perceived disconnect between pursuing a career in cybersecurity and the ability to make a direct impact through human-centered design. As Ame Elliot of SimplySecure suggests, human-centered design principles could be a critical way to connect one’s highly technical work to helping people. (Garcia & Weingarten, 2015) In many ways, it is a way to humanize the cybersecurity professions, by making it more appealing for prospective female practitioners.

**Workforce Entry**

Many problems arise in addressing the underrepresentation of women in the cybersecurity field at the time of workforce entry and at all levels of workforce advancement. One of the most prominent problems is the lack of statistics about women who have graduated from degree-conferring institutions. (Shumba et. al, 2013) This means it is difficult to track progress and test various interventions. This is complicated further by the broadened definition of cybersecurity in terms of occupations and job titles. With only a rough benchmark of the present state (roughly 10 or 12% of cybersecurity professionals are women according to Frost and Sullivan or the Bureau of Labor Statistics respectively), it is difficult to measure progress concretely. (Suby, 2015) (Bureau of Labor Statistics, 2015) At present, Frost & Sullivan, a consulting firm specializing in growth strategy, projects a shortfall of 1.5 million in the global information security workforce 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” (Suby, 2015).

Much of the research also questions whether women see the direct connection between their formal education and the responsibilities of a position in the workplace. This connection is critical, especially given the mission-driven disposition of female respondents in the Carnegie Mellon case. Women in the field echo this finding: “A graduate from a premier US institution—
said that her education was “strong in theory, light on practice... however, she had to relearn things in a pragmatic way” (Shumba et. al, 2013).

Many confounding factors might explain the frustrating disconnect between education and practice that some women face:

- Women might be seeking jobs that they are overqualified for;
- Women may not self-advocate for responsibilities in the workplace due to fears about “tooting one’s own horn;” or
- The connection between skills gained through formal education and their application in the workplace may not be explicit. (Shumba et. al, 2013)

This disconnect is important due to the factors of success for women in cybersecurity: “Women perceived ‘success’ not just as something measured by certain metrics (such as salary), but also as reflecting recognition for both innovative and visionary functions and routine preventive tasks that were essential to information security” (Shumba et. al, 2013). Moreover, the two most common self-reported metrics of success by women in the field included their reputation among peers and having clients regularly seek their advice on security protection issues (Bagchi-Sen et. al, 2010), again emphasizing the importance of a human-centered focus in cybersecurity.

A 2013 study by Professor Rose Shumba and colleagues echoes many of the research findings from earlier in the talent development lifecycle: prominent barriers to entry in field include lack of computing in K-12 education, perception of male dominance in the field, perceived lack of social component, and societal discouragement of women to pursue STEM fields. (Shumba et. al, 2013) It also points to the current lack of effective mentorship as a hindrance to both workforce entry and advancement.
Case Studies from Other Industries

The findings from computer science programs and other feeder programs for cybersecurity identify several challenges to women’s ability to forge successful careers in the field. However, many other unrelated fields have significantly unbalanced gender representation that has improved over time. This section examines other fields with limited female representation to identify best practices for creating an inclusive industry where women have been previously underrepresented or discouraged from entry. Care will be taken to delineate the differences and similarities between the fields in the case studies and cybersecurity.

Medicine: Radiology

The sheer numbers of women in the medical field suggest huge strides towards gender parity: “Women represent nearly one-third of the total physician population in the United States, this number...is keeping with an upward trend: in 1970, 7.6% of physicians were female.” (Freedman, 2010) However, questions remain about the true equality in the field regarding pay, advancement, and respect in the workplace.

<table>
<thead>
<tr>
<th>Key Findings about the Medical Field’s Gender Gap</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Work/Life balance</strong> drives women out of more intense medical fields.</td>
</tr>
<tr>
<td><strong>Technology and lack of connection to the patient</strong> drives women away from technology-intensive subfields such as radiology.</td>
</tr>
<tr>
<td><strong>Low retention rates</strong> are the reason for the drop off in women’s representation in more senior positions</td>
</tr>
</tbody>
</table>

There are several reasons for increased representation of women in the field. One of the most prominent is the near parity achieved in medical school feeders, with women graduating in nearly equal numbers as men. However, the rise of women in medicine has not lifted all subfields equally: “The proportion of women in radiology has been stagnant for the past 30 years, and that’s unique to radiology, because the other specialties have gone up. This seems weird because radiology is a controllable lifestyle (profession) you’d think would appeal to a lot of women,” according to a fourth year student at the Medical University of South Carolina. (Kaplan, 2015) Therefore, if factors related to lifestyle are largely controlled for in this field, why are so few women pursuing radiology? Researchers analyzed application data to examine
the applicant pool for the field as well as any apparent biases in the residency selection process. They found that female applicants to the specialty were either constant or decreasing.

There are several possible causes for why women do not choose radiology. Some are similar to cybersecurity: lack of exposure, fewer female role models or mentors, hesitance with technology, limited human contact, and long training.

The report finds a familiar disconnect between the intensive use of technology and the ability to see its role in helping people. Dr. Julia Fielding, the chair of the American College of Radiology Committee for Women, bridges this gap succinctly, noting that students can see the importance of the field, yet the medical school curriculum does not: “Over the years, radiology became indispensable. It’s better than any other tool for diagnosing appendicitis… The junior people figured this out. They realized that’s where a lot of the decisions were being made. But the people who make the curriculum feel that radiology doesn’t need to be a required course. I would disagree with that.” (Kaplan, 2015) Therefore, much like cybersecurity, earlier exposure to and emphasis on the impact of radiology training could increase the representation of women in the field.

Law

The legal field parallels the medical field in terms of parity of men and women entering law school. However, the legal field itself is only 34% women. The number of women in the field drops off as more senior positions are examined. (The American Bar Association, 2014)

What are the reasons for this drop off? Similar to cybersecurity, “[the legal field is] a very demanding profession and it does take a toll to meet the expectations of partnership while

<table>
<thead>
<tr>
<th>Key Findings about the Legal Field’s Gender Gap</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Work/life balance</strong> inhibits women from staying the field.</td>
</tr>
<tr>
<td><strong>Sexual harassment</strong> is particularly acute for women in this field.</td>
</tr>
<tr>
<td><strong>Diagnosis of current recruitment and workplace policies</strong> is needed to measure improvement and pinpoint which strategies are working.</td>
</tr>
</tbody>
</table>
taking the responsibilities of a family,” according to Carol Clayton, assistant managing partner at WilmerHale, a firm where a quarter of the partners are women. (Ho, 2011)

However, many challenges exist outside of personal obligations inhibiting the retention and advancement of women in the field. A report on the state of women in the legal profession indicates five main factors for women’s underrepresentation in the field: gender stereotypes, lack of support networks, unfriendly workplace structures, sexual harassment, and gender bias in the justice system.

The report responds to these problems with a five-pronged strategy, which constitute best practices for Bar associations, women’s organizations, and corporate and governmental clients (Rhode, 2001) in creating an even playing field for women in the legal field:

1. **Survey the Current State**: Companies should conduct benchmarking studies to understand current attitudes about gender in the workplace.

2. **Eliminate Biases**: “In Fair Measure: Toward Effective Attorney Evaluation, and a forthcoming manual on Best Practices, the ABA’s Commission on Women in the Profession identifies strategies that can help eliminate gender bias in performance assessments and compensation decisions.” (Rhode, 2001)

3. **Encourage Work/Life Balance**: “Any serious commitment to equal opportunity requires a similarly serious commitment to addressing work/family conflicts and related quality of life issues.” (Rhode, 2001)

4. **Provide Mentoring Programs**: “Although the importance of mentors has often been recognized, the institutionalization of mentoring has lagged behind. For many women, senior colleagues can play a critical role in career development by providing advice, support, and as role models.” (Rhode, 2001)
5. **Combat Sexual Harassment:** Companies should strike the right balance in policy between victim’s comfort in reporting misconduct and ensuring checks against false or unwarranted accusations. (Rhode, 2001)

The drop-offs seen in the more senior legal field positions prevent the achievement of parity at every level: “As much as it’s good to see the progress,” Renee Newman Knake, a Michigan State University associate law professor said, “I still remain troubled that we don’t see a lot of our law graduates staying in the profession.” (Smith, 2012) Retention presents the most critical challenge to gender parity in the legal field, since men and women are entering law school at similar rates. Though the entry rates for cybersecurity professions and feeder schools are harder to measure, this research report will continue to focus on the entry-level.

Additionally, the case for gender diversity in both law and cybersecurity is important in the delegation of resources meant to support women in the field. Polls show that people perceive men and women to have different strengths. However, psychology research cautions this assumption, suggesting that gender only accounts for up to a five percent variation in traits between men and women. Instead, “the most respected recent studies avoid sweeping claims about inherent gender differences, but also acknowledge the role of gender-based experiences and expectations in professional lives.” (Rhode, 2001)
Findings from Expert Interviews

Interviews with nine women in the cybersecurity and technology fields offered a view of the successes, barriers, and best practices for women entering the cybersecurity field. Interview participants represented a variety of experience levels, educational backgrounds, sectors, ages, and types of occupations related to cybersecurity. Appendix II provides a full list of interviewees’ names, titles, and affiliations.

Successes

Interviewees consistently cited mentorship, scholarships, and the prominence of women in leadership, branding, and culture as keys to they or their colleagues’ recruitment and retention in cybersecurity field. Based on anecdotal evidence, there are varying degrees of influence or success for each category based on existing organizational culture and implementation.

Mentorship

Interviewees mentioned effective mentorship as an integral part of retention for both women (and men) in the cybersecurity career field. Constantly evolving technology and rigorous work expectations generate a high-pressure environment across the field, in both government and business. Lieutenant Colonel Jori Robinson, former active duty officer in the U.S. Air Force, and currently a member of the Air National Guard and civilian cybersecurity professional noted the intensive nature of military-side mission, which can require up to 3.5 years of intensive training. Before a mentoring program was instituted, both men and women dropping out of the more complex training programs “left and right.”

However, mentorship programs help all employees stay in the field long enough to achieve more mission-based projects. For many men and women, this was the draw of entering the field in the first place: “The military is doing well with retention [in cybersecurity] because of the types of missions (many of which you cannot do in the civilian sector) and technologies they offer.”

She echoed the importance of mentorship in the similarly rigorous occupations in private industry: At her firm, “junior employees get linked with another developer. The mentor helps
with both technical and career-related questions.” After a few years, mentors help [junior staff] examine whether they would like to zero in on a technical career or a career in leadership or management.

**Scholarships**

Several cybersecurity companies have established STEM-related scholarships in hopes of increasing the number of women in the talent pipeline. Google’s Dr. Anita Borg Memorial Scholarship for Women is one such scholarship. Designed to honor Dr. Borg’s work in “revolutionizing the way we think about technology and dismantling barriers that keep women and minorities from entering computing and technology fields,” (Google, 2016) this scholarship provides a financial award for undergraduate and graduate women in technology fields. Scholarship recipients also attend a weekend retreat at Google headquarters.

Parisa Tabriz, Google Chrome Security Engineering Manager and Google’s Security Princess (as denoted on her business cards), was one such recipient: “Scholarship programs are one good way to increase minority representation in the field. I would like to work with my university on programs like this. The world is not equal, and we can’t pretend that it is. [Scholarships] are one way to find and help the talented people who haven’t been given the same opportunities.”

Scholarship programs, stipend programs, and internship programs are all ways that companies can strengthen the pipeline of female students considering cybersecurity careers. Models across companies have varied significantly, however building community through these programs is mentioned as particularly fruitful.

**Prominence of Women in Culture, Leadership, and Branding**

Women are more likely to enter a field where it is clear they “belong,” defined as both seeing others like them and the level of inclusivity in the organization. One key way to meet this goal is to increase the prominence, not just the visibility, of women in culture, leadership and branding. Prominence means that competent women are in key decision-making roles and can advance based on hard work and qualifications. Solely relying on the visibility of women in prominent
positions is not enough. Jewel Timpe of HPE (Hewlett Packard Enterprise) echoes this sentiment, “HPE is run by a woman” and still struggles with a culture shift towards “valuing people based on skills and without bias” as opposed to simply saying “we need more women; we need more people.”

Additionally, the sheer visibility of women in marketing materials and leadership runs the risk of tokenism if competency is not the guiding factor to these decisions. Should women be disproportionately assigned recruitment events and outreach just because they are women? Does this detract from their ability to be competitive within the job they were hired to do? There are several critical ways to avoid tokenism and promote collective intelligence within teams and across the organization:

1. “Combine average ability with complementary diversity of perspectives and expertise to maximize team performance.” (Bohnet, 2016)
2. “Include a critical mass of each subgroup to avoid tokenism” (Bohnet, 2016)
3. “Create inclusive group processes to allow for diverse perspectives to be contributed and heard, for example, by introducing unanimity rules or political correctness norms.” (Bohnet, 2016)
Barriers

Interviewees mentioned several cultural and organizational factors contributing to their challenges when seeking cybersecurity positions. For many, these challenges persisted into their careers and became a part of their day-to-day experiences.

Militaristic/Male-Gendered Culture and Stereotypes

“Cybersecurity is not just programmers in hoodies and a series of zeroes and ones,” according to Ann Barron-DiCamillo, Director of the U.S. Computer Emergency Readiness (US-CERT) team, which leads the U.S. Department of Homeland Security’s efforts to improve the nation’s cybersecurity posture. Despite the highly interdisciplinary nature of cybersecurity, the perception of a scrawny, white male in a hoodie persists. As the “Draw a Scientist” research suggests, this is a huge deterrent for those in the talent pipeline who do not identify with or relate to this stereotype.

At a conference session hosted by the New America Foundation in March 2016, Walter Parkes, producer and screenwriter of such cybersecurity-themed movies as Wargames, Sneakers, and Minority Report, mentioned the dominance of hoodie-clad male protagonists (or antagonists) and the dismal representation of women with the exception of typically goth women with pixie cuts. While the tides may shift with the dawn of shows such of Mr. Robot, featuring well-adjusted, competent women in cybersecurity roles (Cruz, 2015), the composition of cybersecurity and its culture still mirrors what is on-screen historically to some degree.

Outside of stereotypes, the well-documented and particularly pronounced “bro” culture in cybersecurity is encouraged at industry conferences, such as DefCon. One woman described her experience being objectified throughout the conference:

“Like the man who drunkenly tried to lick my shoulder tattoo. Like the man who grabbed my hips while I was waiting for a drink at the EFF party. ... I do not have words for how slimy it is that the official security staff were in charge of what was essentially a competition to [objectify] women...” (Schneier, Schneier on Security, 2015)
Some may, therefore, argue women should just avoid the conference altogether. However, as Bruce Schneier, a prominent cybersecurity expert warns, “When you say, "Women shouldn't go to DEFCON if they don't like it," you are saying that women shouldn't have all of the opportunities that come with attending DEFCON: jobs, education, networking, book contracts, speaking opportunities -- or else should be willing to undergo sexual harassment and assault to get access to them. Is that really what you believe?” (Schneier, Schneier on Security, 2015)

As mentioned, another subset of the cultural problems women face in cybersecurity is tokenism. Parisa Tabriz of Google recounted her experience when her classmates found out about her opportunity to intern at Google. A male classmate’s first reaction specifically stood out when “he said something like ‘It’s a lot easier to get an internship as a girl at Google.’”

The lack of engagement of male counterparts at the education stage through to the career-level is something that cannot be ignored: “It can’t just be that the marginalized groups are the ones solving this problem, because they’re often not in positions of power to make decisions,” says Tabriz. Still, Tabriz is happy she helps “break that [cybersecurity] stereotype” and bring others along. However, taking on additional roles in recruiting or organizational branding are “a load of work that you have to say no to at some point because it takes time, and it isn’t what will be what advances me in my [cybersecurity] career.”

Culture change initiatives (especially large ones) can be expensive and time-consuming. However, Dr. Iris Bohnet offers a simple analogy to show how much small changes in language and culture matter. Bohnet comments, “Even if no one else is watching me today, I will be less likely to drop a piece of paper on a clean beach than on a dirty beach. I will infer from what I see what the norms are in this kind of environment.” The same goes for heavily-gendered, offensive, or alienating language. Employees are more likely to perpetuate these exclusionary behaviors when such actions are already considered the norm.
Recruitment

When asked if they could change one thing about their organization’s recruitment practices, many interviewees cited a desire for technical women to have better representation at all company recruiting and education events. While human resources professionals were seen as effective in conveying the organization’s mission and culture, technical cybersecurity professionals desired the opportunity to ‘speak the language’ of computer science or cybersecurity with representatives of a prospective employer. “Being able to see a female recruiter who understands the terminology and can talk to prospective employees about the work in a real way makes a huge difference,” says Jori Robinson. If that isn’t possible, she suggests human resources consider bringing a developer along to recruitment events.

Many interviewees said they see these simple solutions being ignored for reasons related to budget constraints or complacency, but could not overstate their importance. In over seven years in the field, Jen Weedon, a cybersecurity professional formerly of FireEye, says she still hasn’t seen noticeably good recruitment techniques for women in the cybersecurity field, though she says things [on the hiring side] are improving. There is more organizational awareness about the biases and risks associated with hiring strategies that include “five engineers of the same background [serving] on a panel, deciding whether to hire someone without considering that people with diverse backgrounds may give their teams valuable perspectives.”

Bias in the Hiring Process and Workplace

Implicit biases vary across people, however without controlling for these preconceived notions, people will be increasingly likely to hire others very similar to them. This perpetuates the homogenous representation seen in industries like cybersecurity. However, behavioral insights provide many strategies to reduce these biases. Just as the numbers of women in top orchestras skyrocketed when blind auditioning became the norm (Bohnet, 2016), so too can cybersecurity companies reduce their biases in recruitment and assessment. As Anne Madoff, a recent college graduate in computer science, points out, the national average of female computer science graduates over total graduates is at roughly 15-18 percent. (NGC Project, 2016) Therefore, in her view, there is no excuse for companies that cannot claim at least these percentages. The excuses
of a limited pipeline of women in cybersecurity are dangerous and can be used to continue complacency in sub-par recruitment and hiring practices. Rear Admiral Norton echoed the need to “eliminate bias in hiring, whether that’s by having rigid rules about the process (as is the case in the military) or by creating processes that eliminate information about gender or other characteristics in order to look solely at the skills.”

Additionally, while militaristic culture may be a deterrent for women looking to enter the field, the fairness of performance-based initiatives seen in military recruitment and hiring should be replicated. Jori Robinson spent 16 years in intelligence and cyber-related posts in the Air Force. During her time there, she felt her competencies were judged based on “what she could do, not who she was.” However, in the private sector, she felt “women never came across as being alienated directly, rather pay disparity was the problem.” Rear Admiral Nancy Norton of the U.S. Navy’s Pacific Command is the Director of Command, Control, Communications and Cyber also found the merit-based approach to be advantageous.

**Branding**

An organization’s brand includes everything from marketing materials to interactions with staff or perceptions inside and outside of the market. **Gendered Language:** Language reflecting the experience, prejudices, or orientations of one sex more than the other <gendered language>; also: reflecting or involving gender differences or stereotypical gender roles

How firms frame job announcements can make a large difference in the applicant pool that a job announcement generates. For example, each of the two statements below pertain to cybersecurity. However, they hold vastly different connotations and will likely resonate differently with different demographics:

*Defend against intruders and security threats.*

*vs.*

*Create a safer, more effective networks.*
Jewel Timpe of HPE (Hewlett Packard Enterprise) recounts her experience in working with a cybersecurity firm seeking to increase the representation of women. She was stunned that there were no women in staff composite to start. Moreover, the company website boasted an alcohol-fueled, work-hard play-hard mentality. This was coupled with the company’s hardline initiative that they were only going to hire the ‘top 5%’ of the field. The juxtaposition of this statement with all male branding sent an unintentional but clear signal of a male-driven culture in the cybersecurity industry, and moreover the perception of limited space for women in its top echelons.
Harvard Women in Computer Science Data Analysis

In 2015, the Harvard Women in Computer Science (WiCS) club conducted a survey of roughly 700 undergraduate students without controlling for major, gender, or background in any way. The only incentive to complete the survey was a gift card prize, leading to a random sample of Harvard College undergraduates. Due to small sample sizes and to protect the anonymity of survey respondents, there was a limited ability to conduct analysis on those interested in cybersecurity specifically. However, many of the findings from the Harvard sample echo the qualitative and quantitative findings found in the Carnegie Mellon study. The full set of survey questions can be found in Appendix III.

Findings

In general, when asked about perceptions about the computer science field, there was limited reference to gender specifics in the free-form response to ‘Name three words that describe computer science.’ Students responded in ways that mimicked some of the stereotypes of cybersecurity mentioned across several expert interviews: "smart," "sleep-deprived," "nerdy," and "hardworking".

Still, in examining other free response sections, it became clear that the gender gap has an impact on the student experience for both men and women, though it is decidedly more pronounced for women:

"I don't always feel completely a part of the CS community, or sometimes even taken seriously by others in the community." – Female respondent

"[The gender gap does] Not [have] a huge impact, since some of my best friends who take CS are girls." – Male respondent

"I haven't had any experience in CS at Harvard yet, but I think there's a lot of support for females in CS (ie. WiCS) so I'm not too worried about my future experience." – Female respondent
"Well it doesn't affect me at all. I don't take classes based on their demographic representation; I take them for the material, quality of professor, and to some degree the intelligence/engagement of the student body. None of these things depends on how many women are in the class. I can see how it might discourage some women from taking the more male-dominated classes though." – Male respondent

"It [the gender gap] adds the pressure to excel in CS" – Female respondent

The sentiment about additional pressure as well as a hesitance to speak up in class due to the gender gap was echoed by 2015 Harvard College graduate, computer science concentrator, and founder of the Harvard Women in Computer Science group, Anne Madoff:

“I came to Harvard with the millennial mindset that the glass ceiling wasn't a problem, especially since the numbers of women in computer science at Harvard are double the national average. Still, I felt really isolated and weird and strange pressures – feeling like I didn’t want to speak up in section, because if I was wrong, that would reflect poorly on all of the female students in the department.”

Four years after Madoff cofounded WiCS on Harvard’s campus, women are beginning to feel more confident: "There is actually a pretty strong representation of women here who are CS so I think the gender disparity will disappear soon as more women go into the field and more career opportunities are geared at attracting women to CS" said one female survey respondent.

As shown, male students are much less likely to consider the gender gap in computer science as something that impacts their experience in the computer science department: "It hasn't really impacted my life at all (from only one class), but for a couple of my friends who are female CS concentrators, it seems like something they think about at least a few times week," said one male respondent.
Analysis
Throughout the survey, students were asked to answer questions relating to their gender, the gender gap in computer science classes, their views on computer science as a field, and their confidence in their computer science skills related to their peers. The regression tables pertaining to these findings can be found in Appendix IV.

Perceptions of the Gender Gap in Computer Science
There is a statistically significant relationship between students’ perception of a gender gap and a respondent’s gender. Women were more likely to attribute a higher score to the existence of a gender gap in the computer science department than their male counterparts.

Gender and Computer Science Experience
Women in the sample were also likely to have significantly fewer years of computer science experience than their male counterparts at any given point in their undergraduate experience. On average, women self-reported .73 fewer years of experience than their male counterparts.

Self-Assessment of Skills by Gender
Most tellingly, women reported a lower self-assessment of their computer science skills when controlling for years of experience in the field. Female respondents self-reported lower skill levels (.56 points lower on a 5-point scale, on average) than their male counterparts when controlling for number of years studying computer science.

As shown, Harvard faces many of the same problems that Carnegie Mellon did in terms of attitudes about gender in the computer science department. Computer science is one of many crucial feeder programs for cybersecurity occupations. While cybersecurity is a niche field in many of its feeder programs (law, business, computer science, security, international affairs, among others), the results of this survey can inform and enhance the understanding of why women drop out of cybersecurity-related career trajectories.
Policy Criteria and Analysis

Potential organizational solutions mentioned in interviews and academic research were judged based on the following criteria, derived from New America’s preferences and input from experts in the field:

- **Cost**: The recommendation can be tailored to reflect an organization’s cost constraints.

- **Effectiveness in increasing women’s representation**: The recommendation is effective and tested methods for organizations to use.

- **Measurability**: Organizations have the ability to produce a benchmark of their current state, such that interventions and efforts to increase representation of women can be measured and tested. Data about an organization’s current state should include categories based on inclusive language, culture, branding, and support networks. Interviews, focus groups, or surveys are effective tools in produce benchmark scores.

- **Timeliness**: The projected length of time needed for the intervention may be a factor for organizations given leadership buy-in, staff turnover, or funding cycles.
Recommendations and Implementation

Based on the criteria outlined above, New America should proceed with the following policy recommendations to inform its forthcoming toolkit for businesses and government agencies on gender in cybersecurity. Recommendations are expanded upon below. Scores for each criterion are based on a 1-10 scale, where higher scores indicate higher favorability.

Recommendations are not mutually exclusive and should be pursued together when possible. Additional information about the scoring methodology can be found in Appendix V.

<table>
<thead>
<tr>
<th>Recommendation/Criteria</th>
<th>Cost</th>
<th>Effectiveness</th>
<th>Measurability</th>
<th>Timeliness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessment</td>
<td>5</td>
<td>3</td>
<td>10</td>
<td>5</td>
</tr>
<tr>
<td>Branding</td>
<td>10</td>
<td>7</td>
<td>5</td>
<td>7</td>
</tr>
<tr>
<td>Culture Change</td>
<td>1</td>
<td>10</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>Mentorship</td>
<td>5</td>
<td>7</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>
Assessment

Without a baseline measurement for an organization’s performance in attracting women (or any underrepresented demographic), it will be impossible to measure progress.

Appendix VI offers organizations a simple list of questions to discuss and assess an organization’s level of inclusivity towards women. Additionally, several key mechanisms can inform an organization’s friendliness to women:

- **Retention Rates**: Retention rates are one of the single greatest indicators of health of human capital. (SABA, 2014) In particular, examining the differences between men and women in retention with the organization can show where weaknesses or lack of support are. This is important, not only for the gender divide, but also examining differences in retention rates across types of occupations in cybersecurity. Interviewees consistently referenced that the broad definition of cybersecurity means that not all of the same problems are felt as acutely across different fields. Some interviewees mentioned that they have seen women gravitating more towards policy-based positions than technically-based positions in cybersecurity.

- **Focus Groups**: Conducting focus groups of men and women within the organization can provide a qualitative basis for the success of an organization’s ability to attract and retain talent. Key questions for focus groups might include the following:
  
  - How does your organization bring in all talent? Do these strategies disproportionately help or hinder women?
  - How could the organization design programs to attract women of diverse backgrounds?
  - If you could change one thing about your recruitment experience to this organization, what would it be?
  - What are the most effective things your organization does to attract and retain women? Why are they working? What is not working?

| Cost: 5  |
| Effectiveness: 3  |
| Measurability: 10  |
| Timeliness: 5  |
• How does your organization promote productive conversations in the workplace about gender? How are men brought into the conversation?

• **Anonymous Surveys:** By issuing anonymous surveys, organizations can receive a more candid view of how employees view their workplace. This technique is particularly effective for larger organizations, where larger response rates can ensure anonymity and increased statistical significance. Question design, whether for open response or Likert-scale questions, must be carefully constructed to prevent biasing the responses.

• **EDGE Certification:** Founded at the World Economic Forum in 2011, the EDGE foundation serves as the leading business certification for gender equality in the workplace. EDGE “assesses policies, practices and numbers across five different areas of analysis: equal pay for equivalent work, recruitment and promotion, leadership development training and mentoring, flexible working and company culture.” (EDGE)

• **Industry Benchmarks:** Comparing an organization’s performance with other of similar size, type, and function can produce two key outcomes. First, if the company falls below industry comparisons, a ‘last place effect’ may take hold, prompting an organization to increase its performance to avoid falling further below industry averages. (Kuziemko, Buell, Reich, & Norton, 2011) Additionally, for companies above the industry standard, there is an incentive to continue leading the industry.

The ability to measure an initiative’s success is critical. Many employees struggle to make the case for programs supporting gender equity, especially in organizations without leadership buy-in. Because of this, there is limited funding for gender-based initiatives. Given the opportunity costs for investment, companies should be careful to invest in initiatives that do not offer evaluation or measurement. For example, despite the size of the $14 billion industry of leadership training, general leadership training (trainings that do not size up and correct for lacking competencies of individual participants) consistently lack rigorous evaluation. However, leadership programs that offer to fill a gap in a concrete skills area are more effective. (Bohnet, 2016)

Outside of measuring the effectiveness of interventions such as mentoring and leadership programs, Cecily Joseph, Vice President of Corporate Responsibility and Chief Diversity Officer
at Symantec, echoes the need for more research and concrete examples of what happens with diverse teams. More specifically, it is necessary to demonstrate the return on investment of building these teams: “We need the data to show that this [diverse teams] will produce better products and services.”
Branding

As Jen Weedon, a cybersecurity professional formerly of FireEye, points out, “the field [of cybersecurity] is so diverse and requires many roles outside of coding or programming. People don’t know what ‘cybersecurity’ means.” As many interviewees mentioned, militaristic language at the company level can “dissuade women from applying to the area because [the words] cue that women do no belong.” (Gaucher, 2011) Therefore, the language used by organizations in job announcements, on websites, and in marketing materials is integral to its success in recruiting women. According to interviewees, examining the prominence of women in marketing and branding materials also affects this success.

Language

A synthesis of common words found in job announcements in with strong gender connotations – both in the cybersecurity industry and elsewhere – is included below. (Gaucher, 2011)

<table>
<thead>
<tr>
<th>Common Male-Gendered Words</th>
<th>Common Female-Gendered Words</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Gaucher, 2011)</td>
<td>(Gaucher, 2011)</td>
</tr>
<tr>
<td>• competitive</td>
<td>• warm</td>
</tr>
<tr>
<td>• dominant</td>
<td>• caring</td>
</tr>
<tr>
<td>• adventurous</td>
<td>• comit*</td>
</tr>
<tr>
<td>• autonom*</td>
<td>• empath*</td>
</tr>
<tr>
<td>• challeng*</td>
<td>• interpersona*</td>
</tr>
<tr>
<td>• outspoken</td>
<td>• loyal</td>
</tr>
<tr>
<td>• self-sufficien*</td>
<td>• trust</td>
</tr>
<tr>
<td>• self-reliant*</td>
<td>• understand</td>
</tr>
<tr>
<td>• leader</td>
<td>• yield</td>
</tr>
<tr>
<td>• suffix “-man” ie. “-er”</td>
<td>• communicator</td>
</tr>
<tr>
<td></td>
<td>• the suffixes “-enne” or “-ess”</td>
</tr>
</tbody>
</table>

Organizations should strive to produce job announcements with gender neutral language to increase perceptions of a diverse and welcoming workforce. This serves to increase female applicants’ sense of belongingness, and to avoid deterring women with adequate skill sets from applying. (Gaucher, 2011)
LinkedIn

Language is an unavoidable and endemic part of an organization’s brand. This manifests itself in many ways other than job announcements. For example, LinkedIn is a primary mechanism by which companies are attracting tech talent. LinkedIn typically serves as a key platform for applicants to make connections and apply for jobs. On the recruiter side, LinkedIn provides analytics related to untapped talent (as measured by the number of times a member is contacted by a recruiter) based on anything from geographic location, skill set, education background, years of experience, and more. Cecily Joseph of Symantec cites a diagnostic of her company’s LinkedIn presence as a key way to more deliberately recruit women and minorities to the firm.

By harnessing the analytical power of LinkedIn, companies can more intentionally attract women to their organization. Ann Barron-DiCamillo of US-CERT agrees, “LinkedIn is getting ahead of the curve to encourage people to make the connections” necessary for mobility across the cybersecurity field. LinkedIn also issues regular reports on talent trends for various industries informed by survey data from its users. These surveys are conducted to “to better understand [users’] motivations and behaviors throughout the job search journey,” with a report on “High-Tech” Talent trends coming soon. (LinkedIn)

Scholarships and Continuing Education

Scholarships and continued education programs demonstrate an organization’s commitment to bringing more women into the field. While these scholarships may come with a commitment to work at the sponsoring organization for a fixed amount of time, leaders in cybersecurity, such as Ann Barron-DiCamillo of US-CERT, suggest “continued service at an organization should not be mandatory for [organization-sponsored] trainings. Employees are going to work other places, but organizations need to make sure that they are investing in good cyber talent across the board [regardless of anticipated tenure within the organization].” These investments are not only crucial for an organization, but for the cybersecurity field as a whole.
Culture Change

Culture change must start before any new hire walks through the door. Biases in hiring and performance evaluation hinder an organization’s ability to attract and keep top talent. There are small, tactical choices that can facilitate culture change at the ground level. To minimize the subjectivity of application assessment, the firm should remove personal identifiers from screening materials in order to assess who should be brought in for an interview. (Bateson et al., 2013) Similarly, self-assessments elicit the gender gap in self-confidence (also shown through the WiCS survey data) and such only be considered after assessment from hiring managers or workplace manager.

Moreover, a new employee’s introduction to the company does not stop when the hiring process is over. Key facets of an employee’s first six months in a new position include the language used around the office, the types of projects assigned, and the ability of the company to establish inclusive norms. Following the interview process, it is necessary to create an inclusive office environment to retain talent. Anne Margulies, Vice President at Harvard University, echoed this sentiment, when she overheard a colleague comment to a female engineer that she “didn’t look like an engineer” during a professional meeting. In her view, it is incumbent upon people in positions of leadership to call out this type of behavior, which she did.

As Cecily Joseph of Symantec points out, the “hardest thing is [large-scale] culture change. It is hard to get people to believe that it [culture change] is important and that everyone in a workplace deserves to feel welcome and comfortable.” Joseph says these cultural change initiatives need to be owned at the leadership level, the business unit level, and ultimately, at the individual level. John Kotter and Leonard Schlesinger offer a few key strategies for change initiatives in the face of resistance, adapted in the following table. (Kotter & Schlesinger, 2008)
### Methods for Managing Resistance to Change (Kotter & Schlesinger, 2008)

<table>
<thead>
<tr>
<th>Method</th>
<th>How to Use</th>
<th>When to Use</th>
<th>Advantages</th>
<th>Drawbacks</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Education</strong></td>
<td>Communicate the desired changes and reasons for them</td>
<td>Employees lack information about the change’s implications</td>
<td>Once persuaded, people often help implement the change</td>
<td>Time consuming if lots of people are involved</td>
</tr>
<tr>
<td><strong>Participation</strong></td>
<td>Involve potential resister in designing and implementing change</td>
<td>Change initiators lack sufficient information to design change</td>
<td>People feel more committed to making the change happen</td>
<td>Time consuming, and employees may design inappropriate change</td>
</tr>
<tr>
<td><strong>Facilitation</strong></td>
<td>Provide skills training and emotional support</td>
<td>People are resisting because they fear they can’t make the needed adjustments</td>
<td>No other approach works as well with adjustment problems</td>
<td>Can be time consuming and expensive; can still fail.</td>
</tr>
<tr>
<td><strong>Negotiation</strong></td>
<td>Offer incentives for making the change</td>
<td>People will lose out in the chance and have considerable power to resist</td>
<td>It’s a relatively easy way to defuse major resistance</td>
<td>Can be expensive and open managers to the possibility of blackmail</td>
</tr>
<tr>
<td><strong>Coercion</strong></td>
<td>Threaten loss of jobs or promotion opportunities; fire or transfer those who can’t or won’t change</td>
<td>Speed is essential and chance initiators possess considerable power</td>
<td>It works quickly and can overcome any kind of resistance</td>
<td>Can spark Intense resentment toward change initiatives</td>
</tr>
</tbody>
</table>

To effectively use the change management structures above, leaders and managers must first diagnose the types of resistance they anticipate as they make the case for recruiting, funding, hiring, and culture realignment. For companies in cybersecurity, there is likely an overarching status quo bias given the unique and pervasive culture, not only for specific organizations, but in the field as a whole. Additionally, leaders must examine how to adapt these strategies to the specifics nuances of the organization given size, finances, current composition of the workforce, and the relative power and status of resisters.
Mentorship

Regardless of gender, formal or informal mentors are most successful if they are willing to advocate for the mentee when they are not present. (Bohnet, 2016) This transition from mentorship to sponsorship has been consistently cited as a critical factor for women’s success in the field, both from the perspective as a manager or executive, and from personal experience.

Companies can encourage both formal and informal mentoring programs. One hallmark of successful formal mentoring programs is starting small with a group of enthusiastic employees who will serve as the pilot group, forming norms around meeting frequency, program culture, and expectations. Given already low representation of women in the cybersecurity profession, it is not always necessary to pair women with other women. Rear Admiral Nancy Norton, Director of Command, Control, Communications, and Cyber for U.S. Pacific Command in the U.S. Navy, emphasized the importance of mentorship and sponsorship: “The mentorship piece is very important. It is incumbent on more senior people to… give more junior people an opportunity to show their expertise. [This could be in the form of] assigning a task that hasn’t been asked for. Just because someone isn’t volunteering for it doesn’t mean they aren’t competent to do it.” This is especially true for women with a lower tendency to self-advocate. While Parisa Tabriz of Google does not have formal mentors in the field, she emphasized that “having friends you can trust in the space is important, [because] you experience similar insecurities and micro-aggressions, and it’s important to have peers to turn to.”

For organization that might be hesitant to investment in a formal, long-term program, there are still many benefits to smaller, one-off engagements: “‘Mentoring can be a one-hour mentoring session. We don’t have to escalate it to a six-month or year-long event,’ says Karie Willyerd, [Former CLO of Sun Microsystems, a company that sold computers, computer components, computer software, and information technology services and co-founder of Future Workplace]. Instead of focusing on the long term, think of mentoring as something you access when you need it.” (Gallo, 2011)
Conclusion

The data stored in networks and protected by cybersecurity professionals is valuable and therefore vulnerable. Trusted institutions such as the U.S. government, Target, MasterCard, and others have all fallen prey to these large-scale, damaging attacks. For much of the general public, these breaches and the associated damage control are faceless. However, the largest risks lie not in the breaches seen to date. The current cybersecurity workforce’s headcount is dangerously low. This renders the country unprepared to counter future threats and is exacerbated given the lack of depth and diversity in a workforce that is almost completely male.

To limit the risks associated with the projected shortage of 1.5 million cybersecurity professionals, the field must become more welcoming and appealing to women. There are huge benefits to a more inclusive cybersecurity workforce. The business case for fixing this underrepresentation is not only one of morality or diversity, but one of necessity. Dan Geer, a leader in the cybersecurity industry, observes that cybersecurity is different than other technology fields due to the presence of a “sentient opponent.” (Geer, 2015) This makes the conflict in cybersecurity a talent-based competition, begging the question of why any organization would exclude 50% of the talent pool if beating a sentient opponent is the goal. Anne Margulies, Vice President and University Chief Information Officer at Harvard University, summarizes the stakes particularly well: “[Cybersecurity talent] is a critical need and skillset for companies and the country. Only developing these skills in half of the population is a huge disadvantage.”
Appendices

I. Why is Cybersecurity Different?

Cybersecurity and the challenges of increasing women’s representation in field are distinct from those seen in other STEM fields largely due to how the field was born and started to professionalize.

Jen Weedon, a cybersecurity professional formerly of FireEye, observes that “the trajectory of how the cybersecurity field has evolved explains some of [why cybersecurity is different from other STEM fields]. It has traditionally been focused on computer network defense, with a heavy national security focus and military lineage. Because the field has historically been very defense-oriented, the government was really one of the only places that was training and building the workforce. This means that there are a lot of old timers in the field - former intel and military types that comprise an old boys club.”

According to the National Initiative on Cybersecurity Education (NICE), there is typically a linear trajectory from informal occupations to professions, outlined in the figure to the right. However, according to a NICE report, the cybersecurity field is still in its nascent stages of professionalization and “the effort to professionalize cybersecurity will not be a linear process due to the constant change of technology…The professionalization process unfolds over years or decades rather than over short time periods, and professionalization involves governments, academic institutions, and private sector organizations are involved in the professionalization process.” (Education, 2012)
Subfields and feeder fields of cybersecurity are often further along in the professionalization process:

Differences between Cybersecurity and CS [computer science] also exist within the professional practice of these fields. Computer scientists create systems primarily using their technical skills and knowledge of computer languages and system design. Cybersecurity jobs also involve technical skills such as secure system design and system analysis but they also require knowledge from other areas such as disaster recovery, digital forensics, policy creation, and even physical security. Cybersecurity professional certifications such as the popular CISSP and CISA confirm that security professionals need non-technical background since they test in ten areas including business, CS, and law.” (Shumba et. al, 2013)

The professionalization process can expedite many of the recommendations put forth in this report, as “sticking to the quality control aspect of the report, professionalization, it says, has the potential to attract workers and establish long-term paths to improving the work force overall.” (Schneier, Schneier on Security, 2013) However, given cybersecurity’s unique, fast-paced nature and broad definition, building a diverse community across the field will continue to be difficult. Cybersecurity’s unique trajectory towards professionalization and a heavily-male culture presents organizational problems that could inhibit companies from pursuing the recommendations set forth in this report.
II. List of Interviewees

Anne Barron DiCamillo
Chief Technology Officer
Strategic Cyber Ventures
Former Director

Professor Iris Bohnet
Director of the Women in Public Policy Program
Harvard Kennedy School of Government

Cecily Joseph
Vice President, Corporate Responsibility
Chief Diversity Officer
Symantec

Anne Margulies
Chief Information Officer and Vice President
Harvard University

Anne Madoff
Software Engineer
Mark43

Rear Admiral Nancy Norton
Director of Warfare Integration for Information Warfare and Deputy Director
Navy Cybersecurity
U.S. Navy

Jori Robinson
National Security Fellow
Harvard University

Parisa Tabriz
Google Chrome Security Engineering Manager
Security Princess
Google

Jewel Timpe
Senior Manager, Research Communications
HPE (Hewlett Packard Enterprise) Security

Jen Weedon
Cybersecurity Professional
Formerly of FireEye
III. WiCS Survey Questions: Understanding Computer Science at Harvard

1. Concentration (or best guess)
2. Secondary (if applicable)
3. Graduation Year
4. Prior CS background:
5. Do you have plans to take any CS courses in the future?
6. Are you interested in getting a CS concentration?
7. Have you ever considered taking a computer science course? If not, why not? If you have considered it, why did you decide not to take it?
8. In your opinion, should some programming knowledge be a requirement for graduation? If not, why not? If so, why?
9. Are you interested in pursuing a job with a quantitative focus after graduation?
10. What three words describe a computer science concentrator?
11. What made you decide to take your first CS course?
12. What was the worst part of taking your first CS class?
13. What were your impressions of CS students before you took your first class? After?
14. Do you think you’ll take another CS class? If so, why? If not, why not?
15. What CS classes have you taken?
16. How many years have you been programming?
17. What is your estimated concentration GPA?
18. How good are you at programming compared to others in the CS classes you've taken?
19. How good are you at CS theory compared to others in the CS classes you've taken?
20. How often do you go to office hours on average for your CS classes?
21. How often do you think the average CS student goes to office hours?
22. How accessible are professors in your CS classes?
23. How accessible are teaching fellows in your CS classes?
24. How often do you interact with your CS class course staff?
25. How involved do you feel with the CS community at Harvard?
26. Do you consider yourself a member of any tech student organizations on campus? If yes, specify which ones.
27. How easy is it to find partners to work with on psets or final projects?
28. Are there any specific classes in which finding partners has been hard?
29. How have you met people to work on class material with?
30. I like CS because it gives me a tool to make a difference in other areas I care about.
31. I like CS because I am interested in the CS problems I get to think about and solve.
32. If you are a sophomore, junior, or senior, what did you do last summer?
33. How stressful is the process of finding a summer internship/job?
34. Do you have a role model and/or mentor in CS? If so, who?
35. Do you feel like you need more support in CS from:
36. What three words would you use to describe a computer science concentrator?
37. What will you most likely pursue after graduation?
38. What type of graduate school are you interested in?
39. What subfield in tech industry would you be interested in working in?
40. What gender do you identify with?
41. What race(s) do you identify with?
42. By your estimates, is there a gender gap in enrollment in CS classes?
43. If yes, what factors (related or unrelated to college) do you think cause this gap?
44. If yes, what is the impact of this gender gap on your experience of CS at Harvard?
IV. Regression Tables

There were 708 usable responses in the data set. 56.49% of the sample self-identified as female. Other than the questions about the respondents’ gender, the “Gender Gap” and “Skills” questions were set on a 5-point scale, with higher numbers indicating higher agreement or self-assessment respectively. The “Years” question was an open numerical response. The questions that underlie each variable are included below:

**Gender:** Male (0) or Female (1)

**Gender Gap:** “By your estimates, is there a gender gap in enrollment in CS classes?”

**Years:** “How many years have you been programming?”

**Skills:** “How good are you at programming compared to others in the CS classes you've taken?”

Perceptions of the Gender Gap in Computer Science

```
    . regress GenderGap Gender

Source | SS       | df | MS
------|----------|----|---
Model  | 2.93932222 | 1  | 2.93932222
Residual | 577.122825 | 706 | .817454426
Total | 580.062147 | 707 | .820455653

Number of obs = 708
F( 1, 706) = 3.60
Prob > F = 0.0583
R-squared = 0.0051
Adj R-squared = 0.0037
Root MSE = 0.90413

Gender   Coef.  Std. Err.   t   P>|t|   [95% Conf. Interval]
---------|--------|-----------|----|------|-------------------------
Gender   | .1299675 | .0685398 | 1.90 | 0.058 | -.0045988 to .2645338
_cons    | 3.217532 | .0515177 | 62.45 | 0.000 | 3.116386 to 3.318679
```
## Gender and Computer Science Experience

```
.regress Years Gender

<table>
<thead>
<tr>
<th>Source</th>
<th>SS</th>
<th>df</th>
<th>MS</th>
<th>Number of obs = 150</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model</td>
<td>19.1741147</td>
<td>1</td>
<td>19.1741147</td>
<td>F( 1, 148) = 3.77</td>
</tr>
<tr>
<td>Residual</td>
<td>752.560085</td>
<td>140</td>
<td>5.00407085</td>
<td>Prob &gt; F = 0.0541</td>
</tr>
<tr>
<td></td>
<td>Total</td>
<td>771.735</td>
<td>149</td>
<td>5.17942953</td>
</tr>
</tbody>
</table>

| Gender  | Coef.    | Std. Err. | t     | P>|t|   | [95% Conf. Interval] |
|---------|----------|-----------|-------|-------|----------------------|
|         | -.7391717 | .3806516  | -1.94 | 0.054 | -1.491386 , .0130424 |
| _cons   | 3.765957  | .232582   | 16.19 | 0.000 | 3.306347 , 4.225568 |
```

## Self Assessment of Skills by Gender

```
.reg Skills Gender Years

<table>
<thead>
<tr>
<th>Source</th>
<th>SS</th>
<th>df</th>
<th>MS</th>
<th>Number of obs = 150</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model</td>
<td>22.1836543</td>
<td>2</td>
<td>11.0918271</td>
<td>F( 2, 147) = 18.16</td>
</tr>
<tr>
<td>Residual</td>
<td>89.7896791</td>
<td>147</td>
<td>.610814143</td>
<td>Prob &gt; F = 0.0000</td>
</tr>
<tr>
<td></td>
<td>Total</td>
<td>111.973333</td>
<td>149</td>
<td>.751498881</td>
</tr>
</tbody>
</table>

| Skills  | Coef.    | Std. Err. | t     | P>|t|   | [95% Conf. Interval] |
|---------|----------|-----------|-------|-------|----------------------|
| Gender  | -.5630942 | .1335997  | -4.21 | 0.000 | -0.8271184 , .29907 |
| Years   | .1022544  | .0284894  | 3.59  | 0.000 | .0459527 , .1585562 |
| _cons   | 3.20002   | .1341982  | 23.85 | 0.000 | 2.934814 , 3.465227 |
V. Scoring Methodology: Policy Recommendations

Policy recommendations were scored on a 1-10 scale with higher scores indicating higher desirability. For example, a ten in cost denotes a highly cost-effective solution. A low score in a category such as timeliness indicates that the option will take a lot of time to implement.

While the scoring of these options is inherently subjective and may change based on the size and nature of an organization, care was taken to ensure generalization given different variables such as organization size, resources, and leadership buy-in.

<table>
<thead>
<tr>
<th>Option</th>
<th><strong>Low</strong> Score: 1-3</th>
<th><strong>Medium</strong> Score: 4-6</th>
<th><strong>High</strong> Score: 7-10</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cost</strong></td>
<td>Recommendation represents a serious financial or human capital investment on the part of the organization</td>
<td>Recommendation is an attainable or reasonable capital investment on the part of the organization</td>
<td>Recommendation is a financially cheap or relatively costless for the organization</td>
</tr>
<tr>
<td><strong>Effectiveness</strong></td>
<td>Recommendation is shown to be minimally effective in increasing the representation of women in cybersecurity</td>
<td>Recommendation is shown to be moderately effective in increasing the representation of women in cybersecurity</td>
<td>Recommendation is very effective in increasing the representation of women in cybersecurity</td>
</tr>
<tr>
<td><strong>Measurability</strong></td>
<td>Recommendation is difficult to measure in an empirical way that would permit a concrete understanding of the return on investment</td>
<td>Recommendation can be measure in an empirical way, however there are still nuances that hinder a perfect understanding of the return on investment</td>
<td>Recommendation can be easily measured in an empirical way that would permit a concrete understanding of the return on investment</td>
</tr>
<tr>
<td><strong>Timeliness</strong></td>
<td>Recommendation will take over a year to implement, execute, and see or measure results.</td>
<td>Recommendation will take six months to a year implement, execute, and see or measure results.</td>
<td>Recommendation will take less than six months to a year implement, execute, and see or measure results.</td>
</tr>
</tbody>
</table>
VI. Assessment of Current State

On Recruiting

- Does your organization have recruiters who are proficient in technical language?
- Does your organization have a “Common Myths about Cybersecurity” sheet?
- Are women present in branding materials?
- Are there portions of the application process (such as code or other samples of previous work) that could be anonymized to minimize bias?

On Language

- Does your organization have gendered language in its job postings?
- Does your organization have gendered language on its website?
- Does your organization have gendered language on its LinkedIn page?

On Culture

- Do employees feel comfortable speaking up or correcting colleagues if presented with inappropriate remarks?
- Does your organization have a dedicated HR person or ombudsperson to discuss workplace culture?
- Does your organization have paid leave policy for care providers?
- Do organization leaders see the value of supporting diverse workplace? How do you know?
- Are there women on your organization’s board or leadership?

On Metrics

- Does your organization collect information about retention rates? Are there significant disparities among certain groups?
- Does your organization send out surveys related to applicant, employee, or manager satisfaction? If so, are there questions that relate to gender? How often are surveys conducted? Are the results disclosed in any fashion? Who is responsible for the survey?
- Does your organization have transparent data related to pay? How is pay determined? Are there pay scales or structure that correspond to the duties of a job? Are there significant pay disparities between men and women conducting the same work?
VII. References


Bateson et al. (2013, November). *When Hiring, First Test, then Interview*. Retrieved from Harvard Business Review: https://services.hbsp.harvard.edu/services/proxy/content/44716317/44723760/1e92b58bb1d8f0d9d8ca58bdbf2fbeb6c


