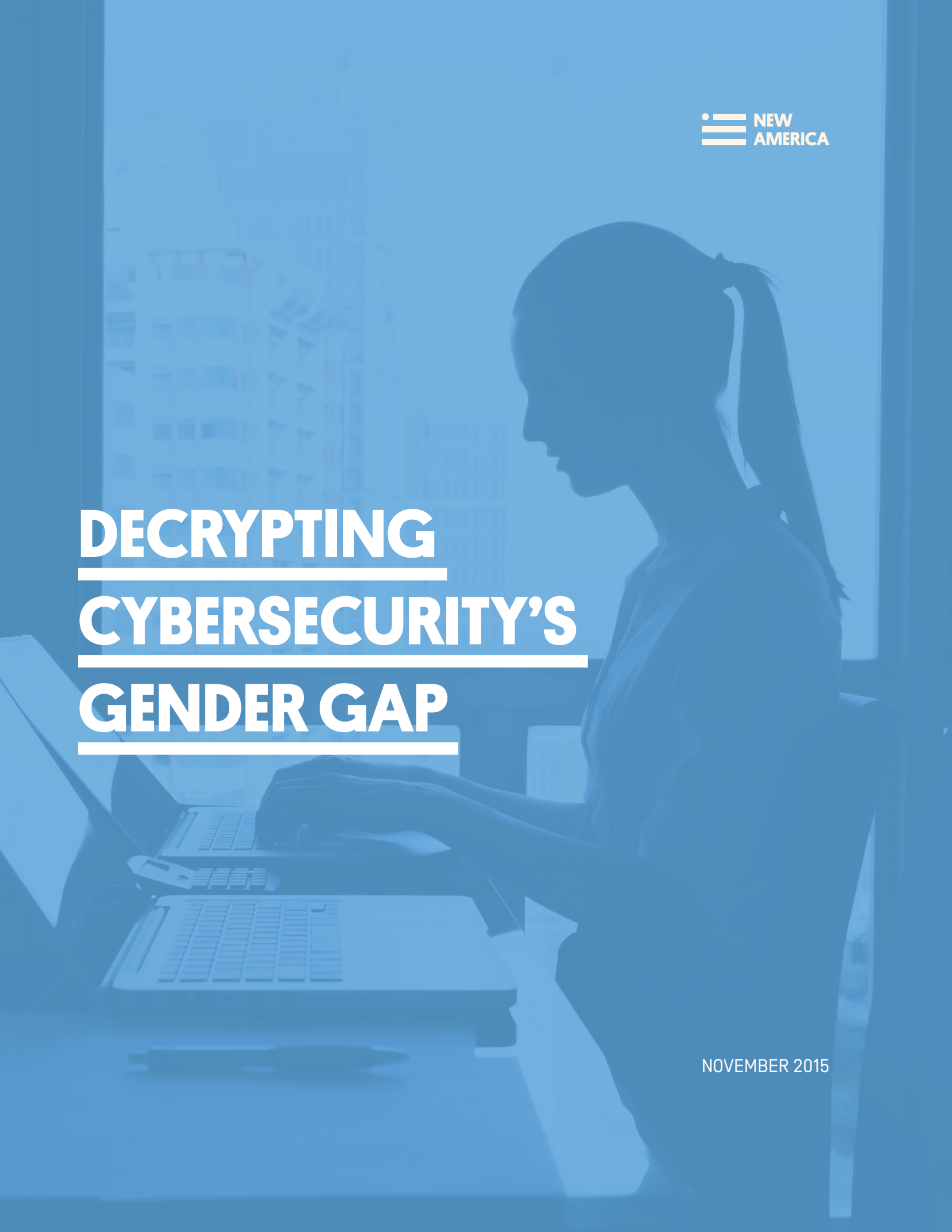
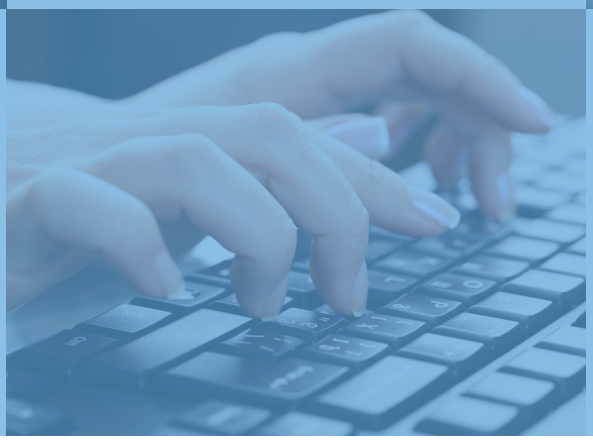


NEW AMERICA

DECRYPTING CYBERSECURITY'S GENDER GAP

NOVEMBER 2015



GENDER DISPARITY IN THE CYBERSECURITY INDUSTRY ISN'T JUST A PROBLEM FOR WOMEN

It's a major national security issue that leaves our businesses, economy, and critical infrastructure susceptible to attacks. In other words, our lack of women and shortfall of talent is a vulnerability we can't afford to ignore.

We've assessed the problem using the NIST cybersecurity framework. Our findings—culled from research and interviews—are within.

1 IDENTIFY

What are the contours of this risk—and what are the impacts on business?

Say the words **"gender gap"** or **"gender parity"** in a boardroom and you're likely to see some eyes glaze over. Narrowing the gender gap was, for a long time, an issue rooted in ethics, justice, and morality. It still is—but there's another big reason to pay attention to the cybersecurity gender gap. It's a major threat to the security of any American who uses the Internet, and any business with digital operations. That's because as more of our personal information migrates to the cloud and global cyber threats continue to evolve and multiply, we will need more and more cybersecurity professionals working across industries. Without more women, the industry will face a major talent shortfall to the tune of 1.5 million in the next five years.[1] Today, women make up only 10 percent of the information security workforce.[2]

Breaches can be poison for any business that collects personal information from its clients and is trusted to keep it safe. According to Bloomberg News, Target said that its U.S. sales were "meaningfully weaker" after it revealed its 2013 credit card data theft. Premera Blue Cross, Sony, Home Depot, and JP Morgan have all reported major data breaches in the past couple of years.[3]

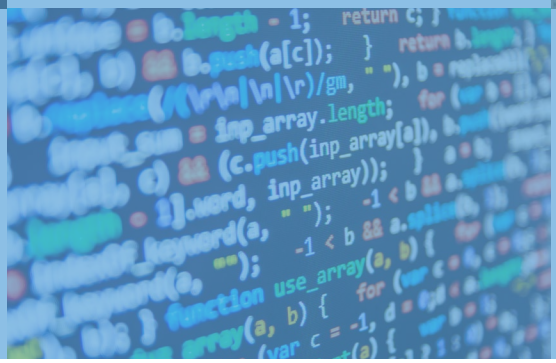
"Signs of strain within security operations due to workforce shortage are materializing," says a recent report from (ISC)². "...the net result is that information security professionals are increasingly cornered into a reactionary role of identifying compromises, recovering from mistakes and addressing security incidents as they occur rather than proactively mitigating the contributing factors."

2 PROTECT

How are misconceptions about the field leaving us vulnerable? One of the biggest reasons that this gender gap exists is due to misconceptions and a lack of awareness about what cybersecurity is, and who can be a cybersecurity professional.

Misconception 1: Cybersecurity professionals are young white guys who eat, breathe, and sleep coding.

Let's be honest: When women (and men!) think of cybersecurity, many tend to think of a young, white, basement-dwelling and hoodie-clad guy hacking into computers. Perceptions like this can be powerful deterrents for young women thinking about entering the field. For decades, researchers have studied how young students' perceptions of what a scientist looks like (through prompts to "draw a scientist") can influence whether or not they choose to pursue a career in STEM. Most students draw the same individual: a Caucasian man in a white lab coat—and this persists "across age groups, grade levels and decades."[4] Both media and professors can reinforce this image, the researchers pointed out. And



the impact of perpetuating this stereotype is clear: Students that carry this stereotypical perception are less likely to take science classes and become a scientist. In 2013, researchers studied this perception problem in computer science, and found that students had similarly stereotypical images of a computer scientist—male, white, bespeckled, antisocial, brilliant, and singularly focused on computers.[5] Since women can't see themselves in this stereotype, they are less likely to pursue computer science careers.

Misconception 2: There is a typical cybersecurity job.

Many women may not realize that cybersecurity jobs need not be at tech companies or even be traditionally "technical." All industries have a need for cyber professionals and cyber work is often as much about the human impact as it is about the technology. **Sometimes, the most important skills to be successful in a cyber job aren't even tech-related.** In a 2013 survey of IS professionals, "communications skills" ranked first in importance to "contributing to being a successful information security professional."[6] In a 2015 survey, communication skills tied with "broad understanding of the security field" as the two most important skills.[7]

Misconception 3: Women don't bring anything different to the table.

"Women in security, as a group, have a more diverse academic background than men," says the study Agents of Change: Women in the Information Security Profession.

"Women tend to think more macro about issues instead of thinking about a particular problem in a microcosm," says Tiffany Jones, the SVP and CRO at iSIGHT Partners. "Women tend to be good analysts because they're able to think from many different perspectives," and to multi-task, a capability that stems from what is a common experience for many women: the need to balance multiple roles and responsibilities—work, family, and kids—all at once.

Because women can be more vulnerable to certain types of cybersecurity threats,[8] it follows that women working in cybersecurity may sometimes be more attuned to that vulnerability and those experiences.

What happens when women aren't at the table? One technology company was experimenting with two-factor identification systems, and decided that in order to log into a system, the user would need to have a particular item in close proximity to the machine. They decided to use a ring for this—so that if the ring was in close proximity to the machine, you could log-in. They didn't stop to think about whether a woman would want to wear a ring that she didn't pick out. The bottom line: arrowing the gender gap is as much about building products and software that work for everyone as much as it is about social justice.

AN ATYPICAL CYBERSECURITY PATH

DANIELLE KRIZ

Think you need to be a programmer in order to succeed as a cybersecurity professional?

Danielle Kriz is living proof that you don't need a degree in computer science to join the cyber ranks. Kriz's educational background is in politics, international trade, and policy. She parlayed that expertise into 18 years of developing trade and e-commerce policy for the high-tech industry inside the U.S. government and corporations. Then, she built the Information Technology Industry Council's global cybersecurity practice.

Kriz's diverse perspective helped her see that that cybersecurity was "a tool for economic growth. If people feel confident that their personal information is secure in their bank or in an online e-commerce transaction, they are more apt to use them. You couldn't have the Internet and global e-commerce if you didn't have cybersecurity." Her global lens has allowed her also to dispel a misperception that cybersecurity is important just for the developed world.

The repercussions of a cyber attack, she says, "aren't just on the hipsters with their mobile phones" but may also affect women in developing countries who use online banking to store funds received through micro-lending services, or farmers in India who use their phones to check crop prices.

CHOOSING BETWEEN WORK AND CARE

CHERI MCGUIRE

Over her impressive career, **Cheri McGuire** has held many positions often requiring long hours and dedication—vice president, chairwoman, board member, director, and … only grandchild. That last one proved to be one of her most challenging roles, in part because of the nature of the cybersecurity industry. McGuire, who is currently the Vice President of Global Government Affairs and Cyber Security Policy at Symantec, first bumped up against the round-the-clock demands of the cyber workplace while in a senior position at the U.S. Department of Homeland Security in 2007.

"I was in a 24/7 cybersecurity operational role, and my grandmother had Alzheimer's and was rapidly deteriorating," McGuire recalls. "She was literally a mile up the road from my office at a facility that specialized in Alzheimer's, but I was only seeing her once every two weeks because of the pressures of my job."

McGuire was torn. She loved her work but soon realized "my career would always be here, and my grandmother wouldn't." So at age 40, McGuire decided to move to a less demanding role in the private sector that would allow her time to balance her second job as caregiver for her grandmother.

In all industries, the forced choice between work and care is more common for women than men, as they still bear responsibility for a larger portion of care work. While McGuire says she has no regrets now about her decision, she wishes there "were better caregiver support structures in the cybersecurity industry to allow women and men to balance personal responsibilities in a 24/7 workplace. Ideally, we wouldn't have to choose between our families and our careers."

3 DETECT

Monitoring our weak spots. Where are we losing women and why? It's an oft-used metaphor, but an apt one here: the leaky pipeline. Here are the key places where women are seeping out of the cyber system.

Leak 1: Middle schools and high schools.

Starting to recruit women in college is often too little, too late. "When I teach college students ...It already feels like we lost a lot of people," says one computer science professor. "By the time you're teaching college you already start to see the [gender] imbalance pretty starkly." Research shows that middle school and high school teachers can play key roles in shifting perceptions around stereotypical images of what a computer scientist or cybersecurity professional can look like—by introducing students to non-stereotypical professionals in the field, discussing the stereotypes and exposing them to media that challenges traditional images and traits that they may think a cyber professional ought to have.[9] For instance, more women show interest in computer science after they learn that it's a field that can have a communal and human impact.[10]

Leak 2: The workplace.

The culture and policies of a workplace go a long way in recruiting and retaining female employees. Though women will soon become the new majority of breadwinners in America, they are also still disproportionately saddled with caregiving responsibilities—often for both children and aging parents—without the policy supports to balance these breadwinning and caregiving roles. That means a company without parental leave, sick days, or arrangements for flexible or part-time work **may end up losing its women (and men) when they are forced to make a choice between caring for a family member and staying in a job** that can often demand 24/7 attention. A woman may not even choose to work there in the first place without those policies.

In a survey of information security professionals that asked about the most important initiatives for retention of employees, respondents ranked "offering

flexible work schedules" and "supporting remote or flexible working arrangements" towards the top of the list. Women suggested that flexible workplace policies and training opportunities were more enticing benefits than inflated salaries,[11] whereas financial incentives were more important for men.[12]

Women may also be repelled by firms without female leadership at the top, translating into fewer mentorship opportunities. Critically, it's not enough to simply have policies on the books, or even to start a feel-good "women's initiative" (women can be hesitant to join such groups because they don't want to be known as the "female" engineer) businesses must also push for culture change and programs that can broaden awareness across the organization. Take, for example, vacation time. Sure, a generous PTO policy is an important first step, but the critical next question is: Is it culturally acceptable to take that time off? Will taking a week of vacation or parental leave prompt an employee's manager or colleagues to question their commitment to the work? Here, it's important for both employees and managers to know the literature about how PTO can actually increase productivity. "Businesses that urge workers to take time off to relax, recuperate, and recharge typically have lower health care, workers' compensation and turnover costs, and they benefit from higher productivity and employee engagement levels," according to the Society for Human Resource Management.[13] [14]

As New America Breadwinning and Caregiving Program Director Brigid Schulte wrote in CNN, "leisure is the new productivity...Psychologists John Kounios and Mark Beeman have mapped brain waves and found the 'a-ha' moment comes in a calm, relaxed state, when we are doing anything BUT work...when we are idle, in leisure, our brains are most active, the Default Mode Network lights up, which, like airport hubs, connect parts of our brain that don't typically communicate. So a stray thought, a random memory, an image can combine in novel ways to produce novel ideas."

Leak 3: The hiring process.

A recent report from the Anita Borg Institute suggests that companies have a few major blind spots when it comes to hiring: Recruiting from a small number of venues, using narrow recruitment criteria (i.e., need someone with a computer science degree), and other hiring processes that may promote implicit biases (using gendered language in job descriptions or screening candidates for "cultural fit," often a way to weed out female candidates). What's more, companies that hire people to do cybersecurity policy often look to the NSA, the DOD, and the DHS, because of the misperception that cybersecurity is fundamentally about defense and warfare. But because those agencies are male-dominated, targeting recruitment there may lead to a majority of male applicants.

"Cybersecurity means different things to everyone…there's not a unified picture of who or what the threat is," says Josephine Wolff, assistant professor at the Rochester Institute of Technology. "So if you leave out a large demographic from the people who are making those decisions…you lose that richness of perspective on what all the threats are that you might want to be protected against."

4 RESPOND

Take action. What are some of the most successful strategies to recruit and retain women?

At school:

- Change the way the field and jobs within it are described. Female students are receptive to hearing about the social context to solving cyber problems—they want to hear about the human side of cybersecurity and understand that what they're doing has an impact on real people.
- Design introductory college and high school classes that would speak to what we've seen to be the interest of female students—the human-centered approach.
- Introduce students to women in the cybersecurity field, and mandate that they read stories that challenge the stereotypical idea of what a cyber professional looks like (this is one of the ways that Harvey Mudd College President Maria Klawe bumped the numbers of female computer science majors there from 10 percent to 40 percent in four years).[15]
- Implement programs that help professors and teachers become more aware of their own unconscious biases and tendencies to treat male students differently from female ones.
- Think about the way classrooms are decorated and designed—posters of male-dominated hobbies and pop culture like Star Wars and gaming—may immediately make women feel like outsiders.

At work:

- Change the way that jobs are advertised (excising gendered words like "assertive," "outspoken," "ambitious," or "collaborative").
- Revamp company policies to make them more conducive to combining the roles of breadwinning and caregiving. Have leaders demonstrate that using the policies is a good thing by taking vacation time or parental leave themselves.
- Hire women at the top who can attract more women coming through the interview process.
- Set concrete targets and goals around increasing diversity so that both employees and the general public can hold the company accountable. Measure hiring managers and leaders against those goals.
- **Create your own talent pipeline in the form of an internship or scholarship program**—reaching out to high schools and universities to find talent early.

CREATING A TALENT PIPLELINE

FIREEYE'S IGNITE INTERN PROGRAM

Why waste time worrying about the shallow talent pool when you can build one of your own? FireEye focuses on growing its own feeder pipeline—starting as early as high school—by recruiting students into a summer internship program.

Often, students commit to two or three summers of internships, "and if they love us, I want them leaving the year before they graduate from university with a commitment from FireEye," explains Barbara Massa, the Senior Vice President of Global Human Resources at FireEye. "Companies sometimes wait to go after graduating college seniors, but then they miss the opportunity to build a relationship with that student over several summers, helping them grow, and leaving an impression of how important and valuable they are to you."

One of the ways FireEye does that: by offering students real and impactful projects with expected deliverables. In 2015, 30 percent of the interns were women, up from 27 percent the previous year.

While they aren't focused solely on recruiting women, they do make an effort to build relationships with diverse affinity groups across campus, casting a wide net in order to eventually "get more women at the executive level, board level, and in our leadership development program," Massa says.

5 RECOVER

As threats, technology usage, and demographics continue to evolve, how do we build a more resilient and adaptive cybersecurity industry? Below are research-backed solutions about what brings women into technology fields, many of which were cited during conversations at the Decrypting the Gender Gap convening in Menlo Park on November 13, 2015:

Retool recruitment programs so that they target mid-career women who are interested in making the transition into cyber. Keep in mind that women tend to be judged based on what they've done, whereas men are often judged on potential. Also recall that women coming from nontraditional backgrounds can contribute as much as those with computer science degrees - and that an ability to communicate clearly is consistently ranked among the top skills needed for success in the field.

Next steps: We need more research on what mid-career women might want or need that differs from those in other talent pools. How might you reach out to encourage them to consider cybersecurity or information security careers?

Reimagine your branding. We know that cybersecurity has an image problem, and that **the pictures we see in media and on company websites make it seem like a militaristic, Cold War-era industry** more focused on coding, systems, and attacks than on people and social impact. Images that cater to predominantly male interests and perceptions of the field can be a powerful repellant for women.

Next steps: Take a look at your website. What does it look like? Does it appeal to women or those without coding backgrounds? Does it include images of underrepresented populations? Does the language sound militaristic or inclusive? Is it written in such a way to suggest that cybersecurity is about securing people and systems? Be sure to review your entire website - not just the part focused on careers and/or the company's commitment to diversity.

Recruit intentionally. There's enough research now to show what works and what doesn't to recruit women - from using more inclusive language in job descriptions to identifying women who do work at your company to be ambassadors to attract others.

Next steps: Ask the women who are at your company or organization why they decided to work with you, what is making them stay, and how they would go about attracting others. Ask them to take a look at job descriptions, and see if they'd consider applying for the job. Use tools like Textio or Unitive to remove gendered language from hiring materials and review applications with names and genders hidden to remove unconscious bias. Send the women who do work at your company to career fairs in order to recruit other women. To counter imposter syndrome - the false sense many women have that they are not qualified for a position if their experience doesn't match up 100 percent with the articulated qualifications - make it clear in job descriptions that not all skills associated with the position are necessary to be considered.

Rethink how we describe and define cybersecurity or information security. **The terms that we use to describe the field, including the word "cybersecurity" itself, can project a narrow definition of what it is**, and one that may not be appealing to women. We need to clarify the full range of jobs available in the field, and emphasize that many of them are about keeping both people and systems safe.

Next steps: Can we create and advance terminology that doesn't elicit political and militaristic images and assumptions? Can we highlight moments in which cybersecurity and information security companies keep people safe? How do we show that cybersecurity affects both systems and people, and is fundamentally a human-centered field?

MEREDITH WHITTAKER, GOOGLE

To understand gender gap,"we need to examine militaristic values that underlie the term cybersecurity"#womenincyber

CECILY JOSEPH, SYMANTEC

"Companies need to better understand & appreciate the business case for diversity in cyber" #womenincyber

AME ELLIOT, SIMPLY SECURE

"I want to bring human-centered design to 'cybersecurity', a term that privileges tech skills" #womenincyber

Retain the women you have. It's not just about creating a "women's initiative" - which can make some employees feel singled-out or sidelined. Make sure there are clear opportunities for advancement, policies that allow both women and men to integrate their caregiving responsibilities with work, and **a culture that encourages employees to take advantage of those policies.**

Next Steps: Conduct an anonymous survey of women at your company to ask about whether they're satisfied with the current policy offerings, and whether they feel comfortable taking advantage of paid leave or flexible work arrangements (if those exist). Are there any programs or workplace rituals that have inadvertently made them feel excluded or uncomfortable?

Retell stories and capture concrete examples about how gender diversity have made a difference in designing software, building a cybersecurity product or brainstorming a solution. This will help to create the larger business case for diversity in cyber - propelling it from a social justice issue to an economic imperative.

Next steps: Start gathering stories and examples that answers this question: What opportunities have we gained because of diversity or lost because we didn't have an expansive view? How have diverse teams impacted user experience or overall design? Highlight the women in your company who are making a difference internally, with other experts, and with audiences you want to recruit.

"We need a culture of experimentation and innovation, allowing employees to try job shares, reduced hours, intense periods on followed by time off, and other possibilities and judge those experiments by the quality of the work that gets done," New America President and CEO Anne-Marie Slaughter said in a Q&A with the Hewlett Foundation about women and cybersecurity.

ENDNOTES

1 Suby, Michael and Dickson, Frank. "The 2015 (ISC)2 Global Information Security Workforce Study," Frost & Sullivan, April 16, 2015. https://www.isc2cares.org/uploadedFiles/(ISC)%C2%B2-Global-Information-Security-Workforce-Study-2015.pdf

2 We don't know how many women work in cybersecurity overall, as the 10 percent number only reflects technical positions, and excludes jobs in legal and marketing departments. This number comes from this report: Suby, Michael. "Women in Security: Wisely Positioned for the Future of InfoSec," Frost & Sullivan, September, 2015. https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/2015-Women-In-Security-Study.pdf

3 Collins, Keith. "A Quick Guide to the Worst Corporate Hack Attacks," Bloomberg News, March 18, 2015. http://www.bloomberg.com/graphics/2014-data-breaches/

4 Finson, Kevin D. "Drawing a Scientist: What We Do and Do Not Know After Fifty Years of Drawings," School Science and Mathematics, Volume 102(7), November 2002, 335-345.

5 Sapna Cheryan & Victoria C. Plaut & Caitlin Handron & Lauren Hudson. "The Stereotypical Computer Scientist: Gendered Media Representations as a Barrier to Inclusion for Women," Springer Science+Business Media, 22 June 2013, 58-71.

6 Suby, Michael. "The 2013 (ISC)2 Global Information Security Workforce Study," Frost & Sullivan. https://www.isc2.org/giswsrsa2013/

7 Suby, Michael and Dickson, Frank. "The 2015 (ISC)2 Global Information Security Workforce Study," Frost & Sullivan, April 16, 2015. https://www.isc2cares.org/uploadedFiles/(ISC)%C2%B2-Global-Information-Security-Workforce-Study-2015.pdf

8 Clark, Katherine. " Sexism in Cyberspace," The Hill, March 10, 2015. http://thehill.com/opinion/op-ed/235070-sexism-in-cyberspace

Miller, Jake. "Report: Anti-abortion Hackers Target Planned Parenthood," CBS News, July 27, 2015. http://www.cbsnews.com/news/report-anti-abortion-hackers-target-planned-parenthood/

9 Finson, Kevin D. "Drawing a Scientist: What We Do and Do Not Know After Fifty Years of Drawings," School Science and Mathematics, Volume 102(7), November 2002, 335-345.

10 Diekman, Amanda et al. "Malleability in Communal Goals and Beliefs Influences Attraction to STEM Careers: Evidence for a Goal Congruity Perspective," Journal of Personality and Social Psychology 2011 American Psychological Association 2011, Vol. 101, No. 5, 902–918.

11 Zakrzewski, Cat. "Women Could Be the Solution to Fighting Cybersecurity Threats," TechCrunch, September 28, 2015. http://techcrunch.com/2015/09/28/women-could-be-the-solution-to-fighting-cybersecurity-threats/

12 Suby, Michael. "Women in Security: Wisely Positioned for the Future of InfoSec," Frost & Sullivan, September, 2015. https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/2015-Women-In-Security-Study.pdf

13 Leonard, Bill. "Employee Vacations are Good for Business," Society for Human Resource Management, July 30, 2013. http://www.shrm.org/hrdisciplines/employeerelations/articles/pages/urging-employee-vacations.aspx#sthash.UASOFXxC.dpuf

14 Achor, Shawn. " Are the People Who Take Vacations the Ones Who Get Promoted?" Harvard Business Review, June 12, 2015. https://hbr.org/2015/06/are-the-people-who-take-vacations-the-ones-who-get-promoted

15 Manoush Zomorodi, "How One College Went From 10 % Female Computer Science Majors to 40 %," Quartz, March 26 2014. http://qz.com/192071/how-one-college-went-from-10-female-computer-science-majors-to-40/

NOTES

NOTES