REPRINT

R&C risk & compliance

# CYBER SECURITY AND THE GENDER GAP: INVESTIGATING ROOT CAUSES

REPRINTED FROM:
RISK & COMPLIANCE MAGAZINE
JAN-MAR 2018 ISSUE




Daubenspeck and Associates

Published by Financier Worldwide Ltd
riskandcompliance@financierworldwide.com


www.riskandcompliancemagazine.com

PERSPECTIVES

# CYBER SECURITY AND THE GENDER GAP: INVESTIGATING ROOT CAUSES

BY **KEN DAUBENSPECK**
> DAUBENSPECK AND ASSOCIATES

Cyber security experts agree that the modern threat landscape is becoming increasingly dangerous. However, the cyber security labour force has been unable to grow accordingly. The field's ever-widening labour shortage creates a significant vulnerability in the modern economy and its overall ability to protect cyber infrastructure is arguably in a state of relative decline. To solve this problem the industry will need to address one of the most persistent labour gaps in the field – the significant underrepresentation of women.

The proportion of women in cyber security is stagnant. According to the 2017 Global Information Security Workforce Survey (GISWS), the proportion of women in the field has not changed significantly since the 2015 survey (11 percent globally, 14 percent in North America) and the UK Office of National Statistics has found no significant increase since at least 2013. To understand why the current status quo results in limited female participation, it is necessary to consider the root causes that may hinder entry into the industry.

## Are women presented with cyber security as a career option?

There is substantial evidence that women are not presented with cyber security as a career option. In a McKinsey profile interview, leading advocates for women in tech suggested that technology is not presented as a normal career path for women.

Research from the Computing Technology Industry Association (CompTIA) supports this. Although CompTIA found that girls' interest in technology lessens as they age, 69 percent of the women who reported disinterest in the industry attributed their attitude to a lack of information about career opportunities.

PwC research has also shown that female students are ruling out tech careers due to the perception that they lack the ability to succeed in the field. Specific to cyber security, a 2013 series of discussion groups held by the Women's Security Society (WSS) found that the industry lacks both defined career paths and information about career entry routes. The majority of participants in the discussions reported that they had "fallen into" their career, and only a small minority had planned to enter the profession in advance.

As far fewer women than men have technology backgrounds, the industry's focus on recruiting talent from science, technology, engineering and mathematics (STEM) fields ensures that most women are not presented with cyber security as a career option. But this focus on STEM talent is unnecessary. IBM's 'New Collar' programme recruits talent based on their willingness to learn instead of their area of expertise, and these talent account for 20 percent of IBM's cyber security hires. KPMG has achieved gender parity in its cyber security division by recruiting equal numbers of people with and without STEM degrees.

Adrian Davis, European managing director of ISC – the group behind the Certified Information Systems Security Professional (CISSP) accreditation, widely viewed as the industry's 'gold standard' certification – believes recruiters are erecting a barrier to female talent by focusing on computing degrees. Not only will recruiting talent from non-tech backgrounds allow more women to view cyber security as a career option, it will also help to alleviate current skill gaps in the field, such as the current lack of CISOs with business skillsets.

## Are employers actively interested in hiring female cyber security talent?

The stagnant level of women in cyber security has become a well-established status quo. This raises a question: has the current status quo persisted despite executives' best efforts or are firms taking a 'business-as-usual' approach to cyber security recruitment? A McKinsey study of non-industry specific workplace trends found that although 74 percent of chief executives said they emphasised gender diversity, only 49 percent of their male employees and 37 percent of their female employees agreed.

The 'business-as-usual' approach remains prevalent in at least one facet of recruitment – the perpetuation of gender-biased wording in job advertisements. Empirical research published in The Journal of Personality and Social Psychology has demonstrated that these advertisements give many

female candidates the impression that the job is not 'for them'. Unfortunately, the use of gender-biased advertisements is common in cyber security due to its status as a traditionally male-dominated industry.

A study for the New America Women in Cybersecurity Project found that "information security organizations and contractors often design male-oriented websites and promotional materials that are not only unattractive but sometimes exclusionary to women". Female participants in the study mentioned "boys club" messaging as a recurring feature of cyber security recruiting pages. A working group study by the cyber security accreditation firm CREST also reported that the industry tends to describe itself in terms designed chiefly to attract men.

Firms may have difficulty deviating from gender-biased recruitment, as it tends to reflect unconscious bias, rather than being a deliberate attempt to cater specifically to men. However, its continued prevalence may indicate that many firms have not taken active steps to root out bias in their recruitment campaigns. Firms can also take actions to compensate for any potential unconscious bias by

explicitly demonstrating an interest in hiring women. These actions include association with professional organisations for women in cyber security, such as The Women's Society of Cyberjutsu, and the use of job boards and ListServs that specifically target women.

Firms are also filtering women out of the talent pool by asking for too many qualifications. Both 451 Research and the Women in Security Society (WSS) have found that recruiters' clients are often uncertain about the qualifications they require. Recruiters have compensated by issuing broad 'catch-all' advertisements that seek candidates with a wide array of technical qualifications. These ads disadvantage female candidates – women are less likely to have all the requested technical qualifications and are more likely to dismiss their eligibility for jobs for which they do not have every qualification listed in a recruitment ad.

It is apparent that some firms are indeed taking steps to address the gender gap in cyber security. However, a substantial portion of firms have maintained a status quo approach and choose to prioritise recruitment strategies that seek a broad array of technical qualifications over strategies that prioritise increasing the amount of applications from female candidates.

## Are cyber security roles attractive to women?

Regardless of what changes are made in the education and recruitment pipelines, the number of women in the field will remain low if potential female talent see it as an unattractive career option. CompTIA research shows that 53 percent of women who have not considered a career in tech would do so if they knew more about their career options. However, for those that do consider a career in cyber security, it is worth investigating whether specific aspects of the field make it unattractive.

> **"CompTIA research shows that 53 percent of women who have not considered a career in tech would do so if they knew more about their career options."**

One factor which limits the attractiveness of tech careers is a lack of role models – the National Center for Women & Information Technology (NCWIT) reports that 30 percent of women in technology fields feel "extremely isolated" at work. Erin LeDell, a software developer for artificial intelligence firm

H20.ai, told FastCompany "The previous company I worked for, I was the only woman there, and after a while, it wears on you". Jane Chwick, Girls Who Code board member and former co-chief operating officer of Technology at Goldman Sachs, has suggested that women do not want to come to a place where they are going to be the only female on the team.

If women are avoiding cyber security careers due to a potential lack of female mentors and colleagues, the result would be exactly the sort of perpetual underrepresentation that we see in the field today. This is why mentorship programmes are one of the most consistently advocated approaches to addressing this issue, particularly as a method of reducing talent attrition. Unless the industry is able to gain a reputation for offering such support, existing perceptions that the field is inhospitable to women will continue to impact recruitment.

Work-life balance is another factor that may reduce the attractiveness of the field to women. Advocates for the recruitment of more women into technology roles consistently stress the importance of flexible work arrangements, but this is a challenge for the cyber security profession. According to Deidre Diamond, founder and chief executive of CyberSN, "When [cyber security professionals] go into incident response mode, [they] might not be home for days, because [they're] working around the clock." Participants in the New America study reported that the long and irregular hours associated with cyber security professions make it unattractive for women with family care giving expectations.

Based on the current state of the industry, work-life balance issues will be an obstacle to many women with families or who plan to have families. Women disproportionately bear primary responsibility for their household and children, and may expect to face informal pushback if they seek flexible working arrangements. As long as the cyber security labour shortage continues, a lack of sufficient human resources necessary to offer alternative working arrangements will ensure work-life balance remains a systemic barrier to attracting women into the field.

## Conclusion

With women making up only 11 percent of the global cyber security workforce, the recruitment of greater numbers of female talent into the industry is a clear way to ameliorate the field's labour shortage. Some barriers to recruitment – such as the lack of clear and normalised paths to technology careers within the education pipeline – are systemic and will take wide ranging and sustained efforts to address. Other challenges can be dealt with more immediately. For instance, firms can readily adapt the practices of industry leaders that have taken a successful interest in recruiting more women. These include recruiting talent without STEM backgrounds and ensuring that recruitment campaigns lack gender bias.

Addressing the gender gap is not a matter of 'diversity for diversity's sake'. The cyber security labour shortage poses an economy-wide risk to cyber infrastructure and data capital. As the cost of cyber attacks continues to climb on a yearly basis, increasing the recruitment of women will help to ensure the continued prosperity and operational success of the modern workplace. R&C

**Ken Daubenspeck**
Chief Executive
Daubenspeck and Associates
T: +1(312) 297 4100
E: info@daubenspeck.com