

Diversity in cybersecurity: It matters

Diversity is more than gender. It is race, culture, ability and country. It is mixing up the talent pool and adding in the unique insights and perspectives that different people from different walks of life bring to create teams that are more engaging and innovative. It will also go a very long way towards filling the very real and very large security skills hole that is growing wider every day. According to Anna Collard, SVP content strategy and evangelist at KnowBe4 Africa, diversity is a critical and strategic step that the cybersecurity industry depends on to ensure longevity and ongoing security capability.



Anna Collard, SVP content strategy and evangelist at KnowBe4 Africa

“Women only make up about 20% of the current cybersecurity workforce and yet one of the top pain points for the CISO is the shortage of security skills,” she adds. “There are four million IT security vacancies that are expected to hit 10 million by 2023, and yet only 1% of cybersecurity senior management are women.”

Research undertaken by Dr Nir Kshetri, professor of management at the University of North Carolina, found that in Africa, only 9% of women make up the security workforce, but it is worse overseas. Women only comprise 7% in Europe, 5% in the Middle East and 8% in Latin America. These statistics do more than just highlight lost potential workforce for the security industry, they also put women at risk, widening the gender gap even more.

“Women use the internet less than men in Africa, and women of colour are more likely to be targeted by hate speech online,” says Collard. “If you are a woman in the public domain, especially if you are a journalist, you are more likely to be harassed online than men. This situation is complex and unpleasant and very likely contributes to the lack of diversity in the technology space.”

There is a need for every part of the technology sector to overcome its inherent bias and to focus on diversity as a whole. The need exists to find ways of minimising the risks and complexities that come hand in hand with women entering the industry. For the cybersecurity sector, this lack of representation also represents an opportunity, one where the skills gap can be addressed at the same time as the diversity one.



New study reveals a surprise finding about digital transformation in SA

29 Jul 2021



“You need different ways of thinking to really deliver next-level problem solving,” says Collard. “In this industry, teams have to think outside the box because this is how the criminals think. It helps to have input and perspectives from different people across different age groups, nationalities, cultures, races and genders. Inclusive and diverse teams are going to be more likely to find unusual or unexpected solutions than those that are made up of the same people from the same background.”

(ISC)² published [Innovation Through Inclusion: The Multicultural Cybersecurity Workforce](#), a report that examined diversity in the cybersecurity workplace across 9,500 US cybersecurity professionals. What it found was that minority women were more likely to hold non-managerial positions and experience pay discrepancies. It also found that racial and ethnic minorities were sitting in the same boat. The report did more than just highlight the unpleasant realities of diversity within the profession, it also found that organisations that had diverse leadership teams saw better revenue, benefitted from a better culture and saw a significant improvement in security posture.

“This situation needs to change, and it needs to change today,” concludes Collard. “This can be done through mentoring programmes that use women to train women, creating spaces that are exciting for women to enter rather than exclusive and intimidating. It can also be improved at the education level by offering cybersecurity as a subject and making it more accessible for all genders, cultures and races.”

For more, visit: <https://www.bizcommunity.com>