Cyber Heroines
African Women in Cyber Defense

InfoSphere
MANAGE. SECURE. TRANSFORM.

AFRICA CYBER DEFENSE FORUM

KnowBe4
Human error. Conquered.

Tomorrow's Cyber Heroines

The importance of attracting young African women and girls to join the cybersecurity industry.

Written by: Anna Collard, SVP Content Strategy & Evangelist KnowBe4 Africa and Aprielle Oichoe, Managing Director Infosphere and Research & Special Programs Director Africa Cyber Defense Forum
Published: February 2021

Photo credit: Omar Lopez Unsplash.com

Cyber Heroines
African Women in Cyber Defense

InfoSphere
MANAGE. SECURE. TRANSFORM.

AFRICA CYBER DEFENSE FORUM

KnowBe4
Human error. Conquered.

Contents

Tomorrow's Cyber Heroines

This report is based on a survey conducted in August 2020 across 445 teachers and educators from 14 African countries. We employed a mixed method descriptive research with the objective of identifying the state of cybersecurity and awareness in the African educational sector as well as challenges and opportunities to attract more girls into the cybersecurity industry.

Background:
Why we need more women in the security industry

"Among the highest likelihood risks of the next ten years are extreme weather, climate action failure and human-led environmental damage; as well as digital power concentration, digital inequality and cybersecurity failure."- World Economic Forum Global Risk Report 2021

Africa's future economic growth, productivity and prosperity depend on her ability to adapt to an increasingly digital and technologically advanced world, a fact that has been further illuminated by the COVID-19 pandemic. However, securing the cyberspace poses a profound challenge to nations and organisations. The Global Cybersecurity Index (GCI) report[1] indicates that there is still a significant knowledge gap in many countries in terms of cybersecurity strategy formulation, cybersecurity awareness, cybercrime legislation, cybersecurity programs, incident response infrastructure and the general capability or capacity to implement all the above. Even before the COVID-19 pandemic, the security skill shortage was listed as one of CISO's top pain points for 2020 across the globe. Globally there are about four million IT security vacancies, according to (ISC)2, and this is expected to rise to 10 million by 2023. (ISC)2 further estimates that to meet the demands of businesses globally, the cyber-security workforce needs to grow by 145%.

According to ISACA's State of Cybersecurity 2020 report [2], 62% of respondents indicate that their organisation's cybersecurity team is somewhat or significantly understaffed, 57% say that some cybersecurity positions within their teams remain unfilled, while 61% believe that fewer than half of all applicants for open cybersecurity positions are actually qualified for the job.

Photo credit: Ayo Ogunseinde Unsplash.com

The acute shortage of skilled cybersecurity talent magnifies nations' and organisations' risk of exposure. And although this skills gap is not just an African problem, the situation is particularly dire on the African continent, where we currently only have a total of about 10 000 certified cybersecurity professionals [3]. Countries like Kenya, which is estimated to have about 1700 security professionals, is only growing by an additional 100 new professionals each year [4].

Cybercriminals have shifted their attention toward the emerging economies, and Africa is a particularly attractive market for them for various reasons:

1. Africa's growth in digitization, leapfrogged by the pandemic and mobile adoption.
2. A relatively immature regulative environment.
3. Low levels of cybersecurity awareness on all levels from government to businesses, and consumers make our continent vulnerable to cybercrime.

According to research conducted by Dr. Nir Kshetri, Professor of Management, University of North Carolina – Greensboro women are highly underrepresented in the field of cybersecurity. Women only make up about 20% of the current cybersecurity workforce globally [5].

The problem is more acute outside the U.S. In 2018, women accounted for only 9% in Africa, 8% in Latin America, 7% in Europe and 5% in the Middle East. Women are represented even less in the upper echelons of security leadership. Only 1% of female internet security workers are in senior management positions [5].

Need for more security awareness is the new normal

With the drastic lockdown measures many countries opted to take, more than three billion people were forced to stay at home. Companies, governments and educational institutions had to roll out remote work technologies and processes that should have taken months to deploy, within a mere couple of days. While nations, organisations and education facilities around the globe are suffused in finding solutions to the COVID-19 crisis, cybercriminals are taking advantage of the expanded threat landscape, lowered defences, disorientation and distraction brought about by the transition to wreak havoc. In a recent survey conducted by VMware, 91% of organisations cited an increase in cyber attacks as a result of teleworking. In their 2020 global landscape on COVID-19 cyber threats, Interpol [6] reports an increase in data-harvesting malware, phishing, and Denial of Service (DoS) attacks and ransomware. Data acquired by Atlas VPN [7] revealed that data leaks surged almost 500% at 27 billion amidst the pandemic, and according to Verizon, confirmed data breaches in the healthcare industry increased by 58% this year [8].

The reason behind more data breaches is multifold. The pace of making remote working a reality was so intense that it resulted in increased human error. IT and security departments faced major disruption and increased workloads as a result of decreased work-forces and distraction from family members and home-schooling. This likely led to security misconfiguration in VPNs, exposing devices to Denial of Service (DoS) attacks or other threats. In addition to this, users had to adjust to working from home without much time for awareness training, often utilising their personal computers or sharing their work devices with family members. The collateral anxiety level we all felt from distractions and increased stress levels makes people more vulnerable to phishing and social engineering attacks -- something cybercrime took advantage of. Pre-COVID-19, cybercriminals were already successfully using social engineering tactics to obtain data and scam people. It goes without saying that if these tactics worked in the standard business environment, they work even better in times of rapid change and confusion. Faced with a larger attack surface than usual during the pandemic, cyber-criminals are capitalising on any opportunity for financial gain.

Photo credit: Shutterstock

Gender gap and the 4th Industrial Revolution

Africa needs more qualified security professionals to protect corporate and national information and create resilience for the post-pandemic world. Including more women in cybersecurity will bring multiple benefits to the security industry itself and better prepare countries for the Fourth Industrial Revolution (4IR).

According to Professor Klaus Schwab, Founder and Executive Chairman of the World Economic Forum, “women will be the most vulnerable when it comes to job losses. Many of the opportunities the Fourth Industrial Revolution will offer are internet based.[9]” Yet, as a recent study has shown, women tend to have less access to internet-based technologies than men do in Africa.[10] This means that the impact on women’s lives and work opportunities becomes a critical concern. If current industry gender gap trends persist, women are at risk of losing out on tomorrow’s best job opportunities. With the increase in automation, those working in “routine intensive occupations” – such as secretarial or call centre work – are considered likely to be replaced by machines. Robots are being prepped to replace care-worker jobs. Women typically occupy these types of professions.

Photo credit: Christina@wocintechchat.com Unsplash.com

The gender digital gap on the African continent more broadly, is only widening, with women having lower digital literacy, less access to internet-based technologies, and less relevant online content than men. This suggests that women may be left out of increasingly digital work opportunities too.

Shockingly, in addition to the above, according to Amnesty International researchers, women of colour were found to be 34% more likely to be targeted by online hate speech than their white counterparts.[11] According to research published by Pollicy "African Feminist Research for a Feminist Internet," 39.3% of African girls were concerned or very concerned about their online safety and have experienced online violence or attacks. [12] And African governments are not doing enough to prevent online gender based violence GBV and protect victims. Most countries across the continent do not have specific legislation, strategies or preventative measures against online gender based violence.

Research by African Feminist Research for a Feminist Internet August 2020 [12] shows that only 36% of respondents had taken concrete steps toward increasing their safety online, and for 80% of those, the major action was to frequently change their passwords. More than half of the respondents have not prioritized internet security at all:

>> "Never thought about it" (25.7%)

>> "No one would take the time to hack my account" (34.6%).

There also seems to be a serious lack of understanding about women's rights in cyberspace, as 86% of the women in Senegal were not aware of policies and laws in place to protect them. In Uganda, this figure was 95%.

Why are women underrepresented in cybersecurity?

According to Shannon Wilkinson, author of "Ripping Off The Hoodie: Encouraging the Next Generation of STEM Girls,[13]" women's lack of involvement and interest comes down to a couple of key factors:

1. discouragement by parents or educators
2. negative stereotypes
3. a lack of role models or mentors
4. low self-confidence or imposter syndrome
5. unconscious bias
6. discrimination and conscious bias
7. fear of competing in male-dominated industries

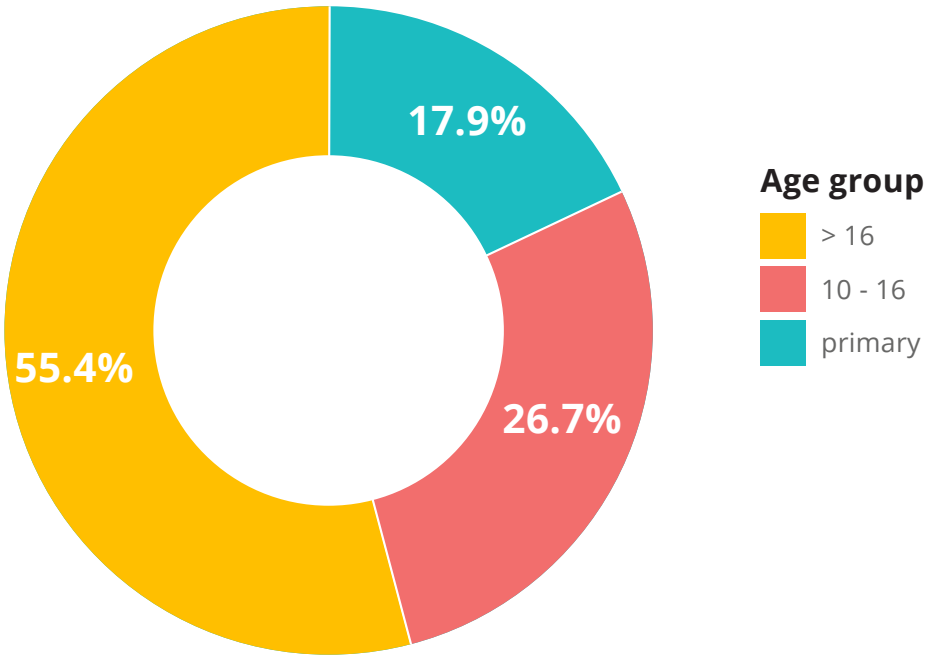
One of the major contributing factors has been attributed to many females being discouraged from getting involved in technology at a young age, thereby reducing the overall pipeline of women with STEM skills.

Encouraging young girls' interest in technology and then continuing to support their interest and education is an important counter strategy to slowly start closing the gap between genders in the workforce.

Survey Findings

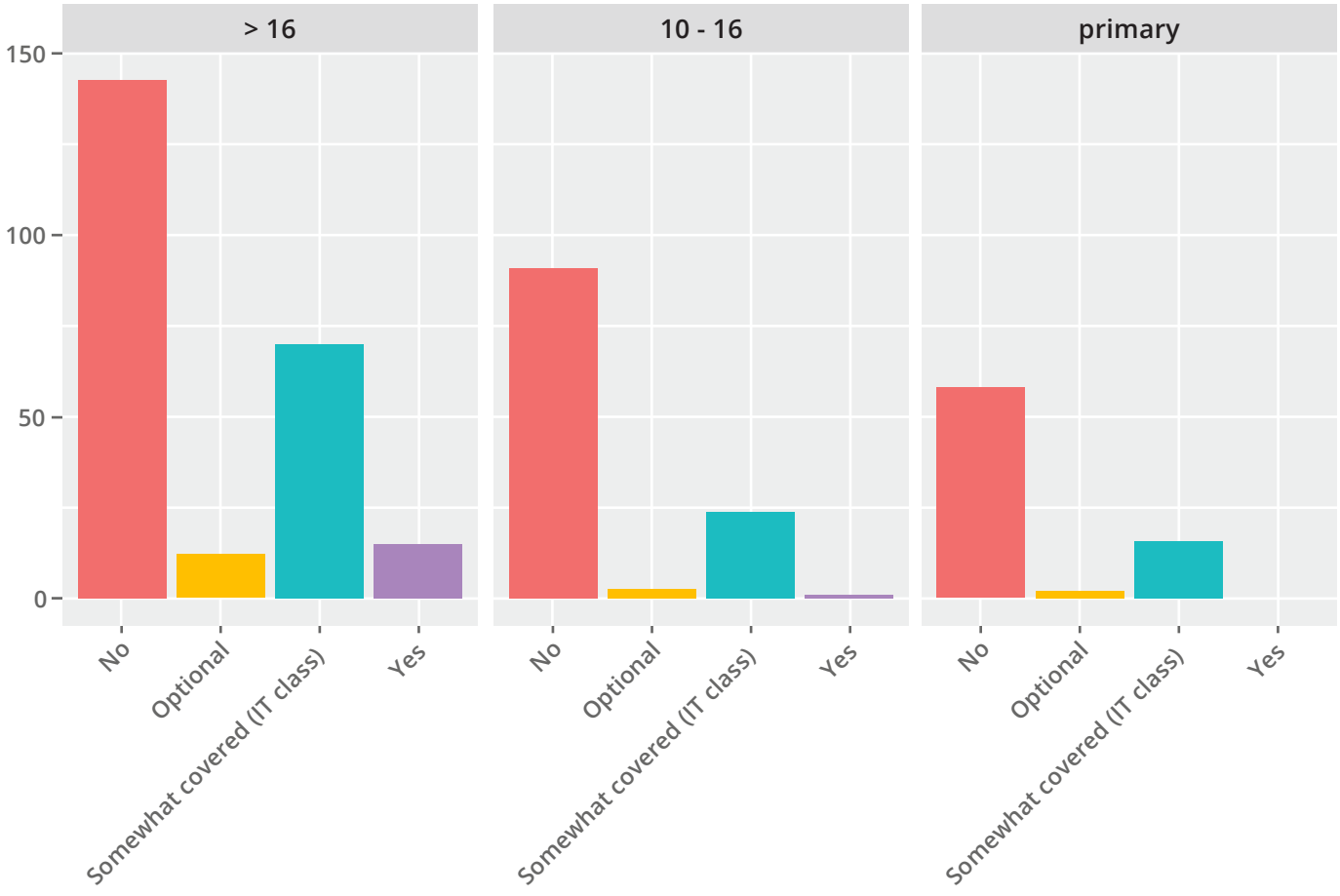
Roughly 32% of the respondents are educators in public schools, while 24.1% are educators in private schools, 17.7% in tertiary education institutions, and 25.5% are educators in other types of institutions. The respondents catered to different age groups, however as depicted in the graph below, we see that the ratio of children below 16 to that of children above 16 is almost 1:1, which means that the efforts put into cybersecurity education in tertiary institutions are not much higher than those put into lower institutions.

Age group representation %



On the question as to whether cybersecurity is offered as a subject in schools, only a paltry 3.7% answered with the affirmative. These 3.7% indicated that it was optional, 25% said it was somehow included in the IT curriculum, but the overwhelming majority of respondents (67.6%) responded that cybersecurity was not taught as a subject. An assessment of cybersecurity teaching across age groups indicated that children in primary school to 16 years received little to no cybersecurity education as depicted below:

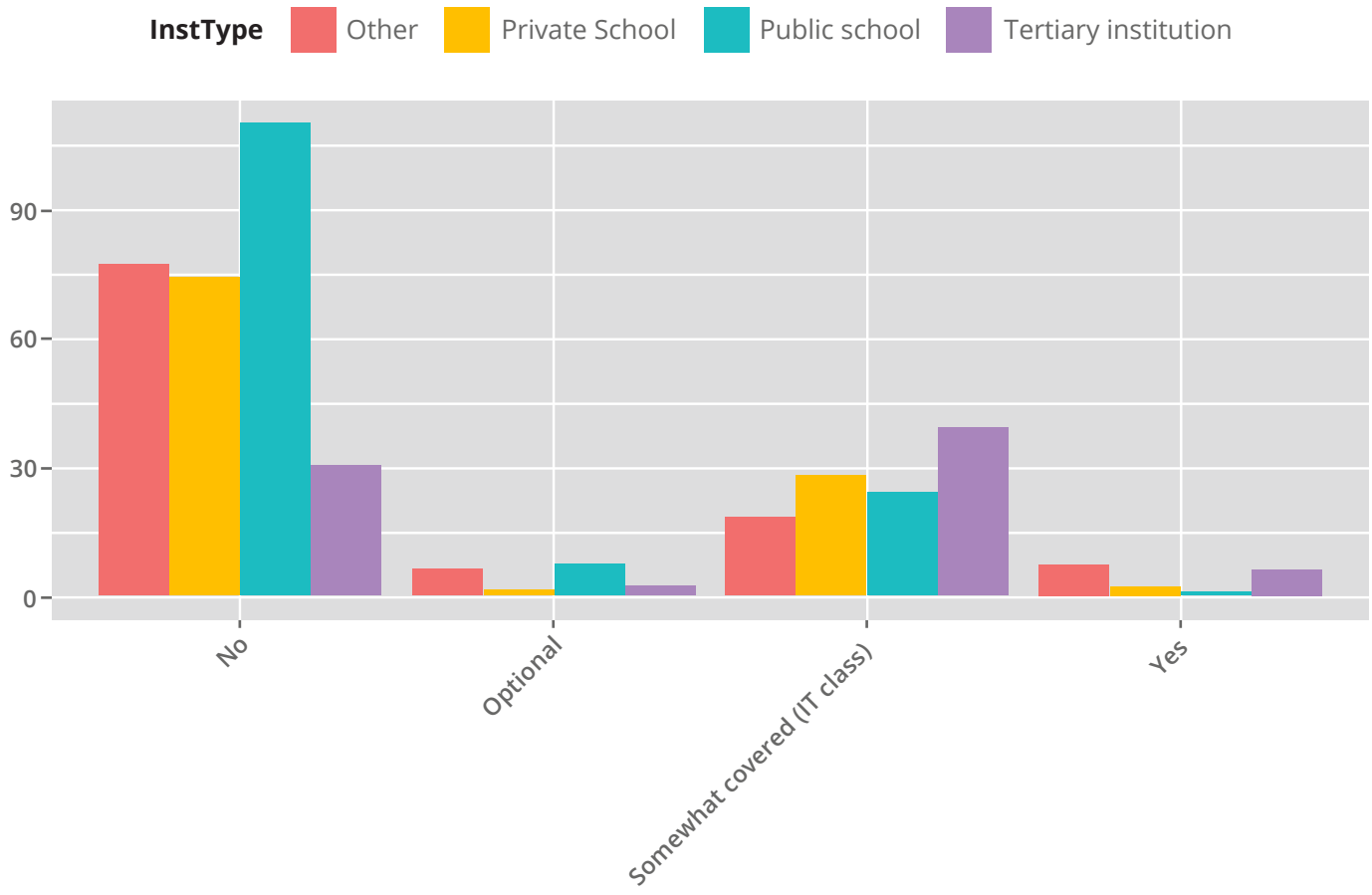
Cyber security teaching across age groups



Cybersecurity awareness in African schools does not fare much better, as 55.6% of the respondents indicated that they did not do security awareness.

An assessment of cybersecurity education across institution types indicated that cybersecurity is mostly taught in tertiary institutions and others that may not necessarily be the regular, mainstream educational institutions. Cybersecurity education in public schools is significantly lacking.

Cyber security in institutions outlook



CS offered as a subject

Suggested initiatives

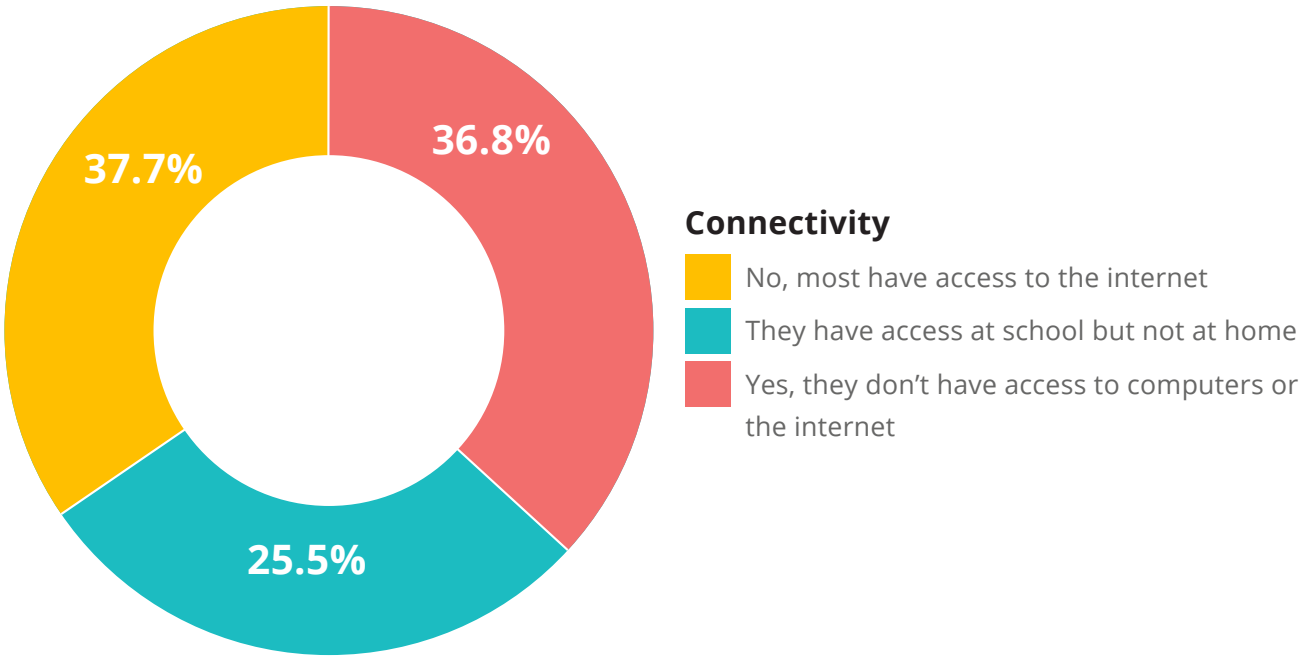
With a predicted deep, global recession, building Africa's human capital through inclusive quality education is the keystone for her to recover from COVID-19 effects and achieve economic growth, productivity and sustainability. More importantly, to help close the gender gap in technology, it is crucial that we encourage an interest in STEM for girls from an early age, dispel the stereotypes of what it means to be a woman in technology, and provide positive role models and mentoring.

Provide content via teachers & online

The feedback from the educators on the ground was eye-opening, as in the African context, we need to be cognisant of some of the unique challenges young people face on the continent. For example, 36.6% of the respondents said learners don't have access to computers or the Internet. Nearly 25% have access at school but not at home.

This requires us to provide access to information via the teachers themselves in addition to direct online content as the access infrastructure is just not available to everyone.

Internet connectivity access challenges



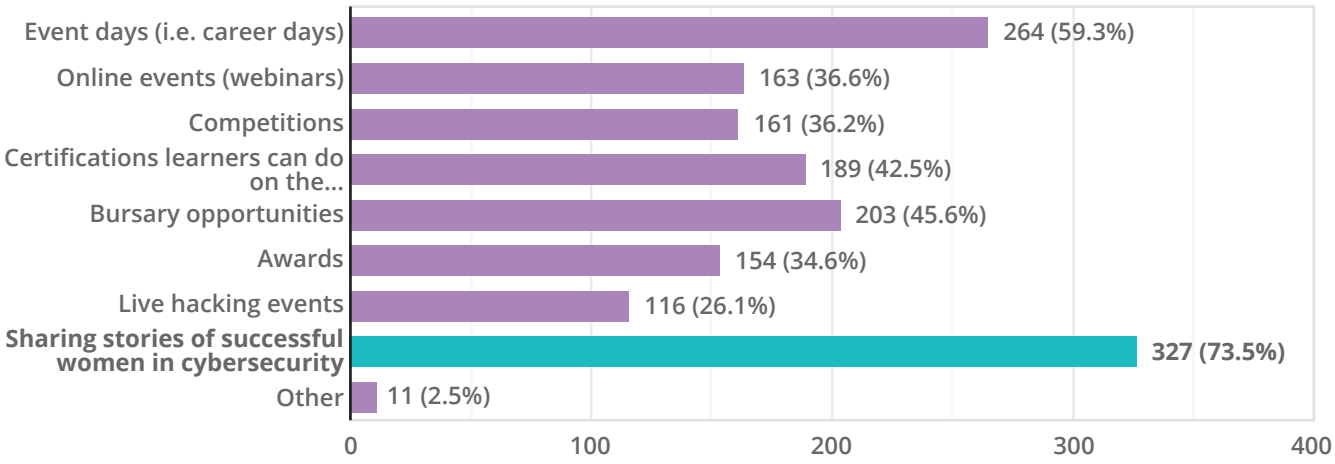
Share success stories

Seventy six percent of the respondents believed that sharing success stories of other (African) women in the cybersecurity space would provide the best level of inspiration.

Career days came second with 59% of the votes, followed by bursary opportunities, online events (webinars) and competitions.

8. What learning interventions would work best in your opinion to attract girls into tech/cybersecurity? (you can choose multiple options)

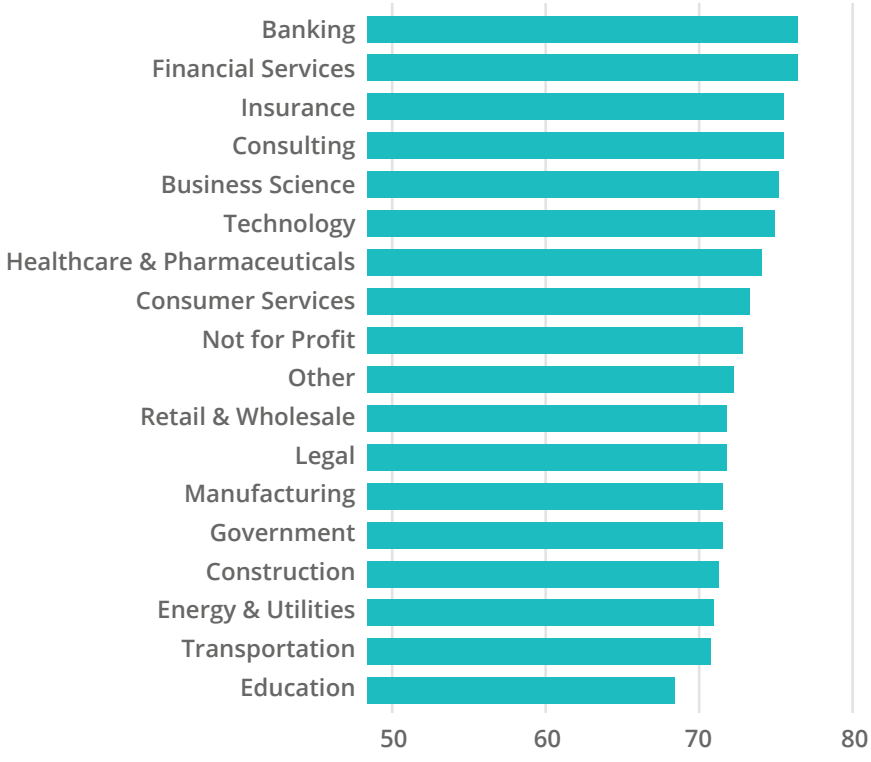
445 responses



Making cybersecurity a life skill & raising awareness

Currently only 20% of schools offer adequate cybersecurity awareness to their learners. Only 25% of schools provide cybersecurity awareness training to their staff and teachers. With the COVID-19 induced, forced move toward online schooling and the use of social engineering tactics by cybercriminals, there is a major gap here that needs to be addressed by the educational institutions. In KnowBe4's 2020 Annual Cybersecurity Culture report, the educational sector scored the lowest regarding cybersecurity culture. This is a global finding and not just limited to Africa.

Figure: Comparing Security Culture Scores.[14]



More needs to be done to increase the cybersecurity awareness levels among schools and tertiary institutions. Governments and educational departments should make basic cybersecurity a core subject for all grades.

Figure: Comparing Security Culture Scores -- KnowBe4 Culture report

Respondents' suggestions

Every respondent provided great suggestions. More than 90% of the respondents opted in to be contacted for further interviews and follow up communication, demonstrating a real interest in solving the challenge of raising interest in cybersecurity among their learners.

Below is a summary of the most common recommendations:

Include cybersecurity in the school curriculum

>> High school teacher, Kenya: "It should be incorporated in the school curriculum, as part of the teaching/learning content. This way it will reach more learners. Also, teachers who are interested in this field, especially women, should be given an opportunity to gain this valuable skill."

>> High school teacher, Kenya: "Through teacher training so that they can teach the learners about it from a young age."

>> Primary teacher, DRC Congo: "Attackers lie in wait for the most vulnerable and attack. Females from as young as 13 are lured into various unconventional activities. With COVID -19, the whole world has been forced to embrace technology, but there is a need to feel secure and safe."

>> Principal, primary school, South Africa: "I teach these more at boot camps, it would be great to have cybersecurity topics integrated into the school curriculum so the younger ones are familiar with it from a younger age. Also, availing internship opportunities as they learn will give them a realistic feel of what a career in security is."

Photo credit: Annie Spratt Unsplash.com

General awareness

>> High school teacher, Mozambique: "There needs to be more awareness created about the online dangers as well as the opportunities which exist in cybersecurity. So, a combination of outreach, role models and tangible practice with the cyber world is important."

>> High school teacher, Egypt: "Intro videos on the topic should also be shared on social media platforms."

>> High school teacher, Kenya: "Sensitize learners of the career by radio, social media and TV adverts."

Remove the fear of math and show role models who struggled with math in school

>> Principal, primary school, South Africa: "Bring the experts to the learners so they become aware of the possibilities. This should happen not during teaching time, but after. The fear of math as a subject is, in my opinion, one of the greatest obstacles in learners' minds when contemplating a career in computers. The stigma around math needs to be broken. An idea is to bring high school or even university students who are excelling, but struggled in school, to the learners and simply talk to them to motivate them to push for success.

Songs & Competitions

>> Primary school teacher, Kenya: "Debating the matter in class first as well as creating songs to inspire learners to find out more about cybersecurity."

>> Primary school teacher, Botswana: "A greater awareness campaign dedicated to attracting them would be great. Song, play, etc."

>> High school teacher, Kenya: "Create an online programme, invite students to engage, have a competition and award the best three with a scholarship."

Female role models

>> High school teacher, Kenya: "What I have noticed is that kids (teenagers) learn and act from live examples they see and from whom they look up to. So, I would say, girls seeing success examples from women in the industry would be a great way to attract them to the cybersecurity industry."

>> High school teacher, Ethiopia: "Role models, talking to experts who have made it in the field."

>> Tertiary institution lecturer, Nigeria: "Pairing industry experts to young talent. I have seen how talent sprouted from this initiative. Get industry experts to publicly share experiences and how cybersecurity transformed their lives, earnings and perception of work."

>> High school teacher, Egypt: "Let them experience it themselves. Inspiration nights where other ladies working in the field give talks of how this path helped them in their lives. Career counseling clinics to help refine what in particular they can do in cybersecurity, i.e.: career path."

Bursary opportunities & online holiday courses

>> Tertiary lecturer, Kenya: "Due to poverty, most of the learners will not be able to afford an education in cybersecurity, so it would be great to offer bursary or scholarships."

>> Tertiary lecturer, Kenya: "Come up with various categories of scholarships in tertiary institutions targeting girls, such as orphans, partial orphans, girls from arid and semi-arid regions, and girls in STEM. Run cyber awareness and marketing programmes targeting girls via radio, tv, and social media."

>> Tertiary lecturer, South Africa: "My daughter wants to study IT at university when she finishes school. I'd love for her to be able to access bursaries and options for study paths. We have attended holiday workshops on robotics and coding, but there has never been anything available to her on security."

Include parents

>> Primary teacher, Kenya: "Start at an early age and include parents and caregivers in the awareness generation. Make it interesting to learners."

Make content age appropriate and "cool"

>> Primary teacher, Kenya: "Provide awareness content that's tailor made for the learner's age group. Make it cool."

Equip girls against online GBV and cyber bullying

>> High school teacher, Kenya: "Inform girls about cybersecurity and how to know if they are bullied, how to identify cyber bullies and to speak out without fear in case they are bullied."

>> High school teacher, Kenya: "Provide forums for women who have overcome the cyber challenge to share their stories and equip and empower women against cyber bullying."

>> High school teacher, Seychelles: "Encourage girls to adopt the independence and go-getter mentality like the boys. Make girls understand that it's important for them to help protect their gender from cyber bullying."

What can you do right now?

It is clear that we need to change the status quo of the gender imbalance in the security & tech industry in Africa. And shifting gender biases needs to start at grass root levels such as primary and secondary schools as well as within our communities and at home.

If you are a parent: become aware of any potentially unconscious gender bias beliefs and try change these within your own inner circle. Gift more science books to girls at birthday parties, make technology sound interesting and fun, encourage girls to sign up for coding or robotics as well as IT and security classes.

If you are currently working in tech or cybersecurity and would like to make a difference, get in touch with your local schools or universities to provide guest lectures or share some insights about your career.

If you are or know of any women in the security industry who would make good role models, please get in touch to be added to our database of cyber heroines. We aim to create a short video profile of each security expert which can be shared amongst schools as role models.

Go to cyberheroines.com or email hello@cyberheroines.com

Photo credit: Suad Kamardeen Unsplash.com

References

1. Global Cybersecurity Index (GCI) 2018
https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

2. ISACA State of Cybersecurity 2020
https://www.isaca.org/go/state-of-cybersecurity-2020

3. Serianu Africa Cyber Security Report - Kenya 2018
https://www.serianu.com/downloads/KenyaCyberSecurityReport2018.pdf

4. Serianu Africa Cyber Security Report -2017
https://www.serianu.com/downloads/AfricaCyberSecurityReport2017.pdf

5. "The lack of women in cybersecurity leaves the online world at greater risk" by Nir Kshetri, Professor of Management, University of North Carolina – Greensboro, 2020
https://www.govtech.com/workforce/The-Lack-of-Women-in-Cybersecurity-Leaves-the-Online-World-at-Greater-Risk.html

6. Interpol Cybercrime: Covid19 Impact
https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

7. Data leaks surge almost 500% at 27 billion amid pandemic" by Alex T. | August 24, 2020
https://atlasvpn.com/blog/data-leaks-surge-almost-500-at-27-billion-amid-pandemic

8. Verizon Data Breach Report 2020
https://enterprise.verizon.com/resources/reports/dbir/

9. https://www.weforum.org/press/2016/01/five-million-jobs-by-2020-the-real-challenge-of-the-fourth-industrial-revolution/

10. African women face widening technology gap by African School on Internet Governance (AfriSIG) - Published on 1 April 2019 https://www.apc.org/en/news/african-women-face-widening-technology-gap

11. #TOXICTWITTER VIOLENCE AND ABUSE AGAINST WOMEN ONLINE - Amnesty International 2018
https://www.amnesty.org/download/Documents/ACT3080702018ENGLISH.PDF

12. Alternate Realities, Alternate Internets African Feminist Research for a Feminist Internet Neema Iyer, Bonnita Nyamwire and Sandra Nabulega August 2020 African Feminist Research for a Feminist Internet August 2020

13. "Ripping Off The Hoodie: Encouraging the Next Generation of STEM Girls" by Shannon Wilkinson 2020
https://www.amazon.com/Ripping-Off-Hoodie-Encouraging-Generation/dp/B08J21KYWC

14. KnowBe4 Security Culture Report https://www.knowbe4.com/organizational-cyber-security-culture-research-report

Cyber Heroines
African Women in Cyber Defense

InfoSphere
MANAGE. SECURE. TRANSFORM.

AFRICA CYBER DEFENSE FORUM

KnowBe4
Human error. Conquered.

Thank you

cyberheroines.com
hello@cyberheroines.com