*Sochin Research Institute*
*Marula Manor, P.O. Box 1927-00502, Nairobi*

***Research Note, updated January 12, 2022***

# Using Cybersecurity as a Tool to Empower Women

**Dr. Rosa S. Ko** [1]

[1] Sochin Research Institute; rko@sochininstitute.org

**Abstract:** This note is based on research conducted for the 5Ws of Cybersecurity grant that SRI received from the U.S. Embassy Nairobi and implemented from October 1, 2019 to September 30, 2021. A data analysis suggests that stereotypes about women in technology need to be critically examined. The findings show that women are just as capable as men and hence need to be offered more opportunities in the cybersecurity sector.

**Keywords:** Cybersecurity, gender equality, empowerment

## 1. Background

Kenya unfortunately has been a tempting ground for hackers committing crimes in cyber space and this calls for tougher policies and regulations. 38.8 million cyber threats occurred in the country between April and June 2021, according to a report by the National Kenya Computer Incident Response Team Coordination Centre. Cyber attacks have real world consequences ranging from identify theft to billions of shillings being lost every year. Moreover, the Communications Authority of Kenya reported that 3 in 4 shillings stolen through cybercrime in 2018 were not recovered. A major obstacle to improving the cybersecurity environment in Kenya is the lack of professional talent and skills shortages among ordinary citizens who go online every day.

Against this backdrop, the Sochin Research Institute received a grant for a cybersecurity project from the U.S. Embassy Nairobi in late 2019. The grant aimed to further the Embassy's strategic goals of strengthening capacity to prevent and respond to threats of crime, to counter violent extremism, and to contribute to regional peace and security, particularly targeting at-risk youth. The project components included in-class training, an awareness campaign conducted on social media, and a public speaker series with cybersecurity experts.

## 2. Project Design

In order to recruit participants for the cybersecurity training, non-probability sampling was used to survey Nairobians between 15 to 35 years old using Facebook. Several keywords were used to target technology-oriented users and a gender-neutral approach was used. Participants were then directed to an online pre-training assessment that collected relevant personal meta-data as well as responses to 12 technical questions. The survey was administered in several phases starting on October 23, 2019 and gathered 1,600 responses by the end of the project. A post-training evaluation also contained 12 questions and having results from both assessments enabled the calculation of the learning effect at both the individual and aggregate levels.

## 3. Key Highlights from the Pre-Assessment Assessment

After anonymizing the data from the pre-training assessment, a multi-linear regression analysis was conducted to determine causal relationships between respondents' backgrounds and their performance on the assessment. Below are key observations from the analysis:

- The average score was seven correct questions;
- 74 per cent of respondents had either an undergraduate or graduate degree though education level had no impact on test results;
- There was no statistical relationship between the four independent variables (gender, educational level, pervious cybersecurity training and age) and the score achieved in the pre-training assessments;
- The median age of respondents was 25 years, which likely implies that most do not have much work experience yet;
- **Respondents performed better with scenario based questions than with theory based ones.**

## 4. Analysis of Training Participants

Participants for the 5Ws of Cybersecurity in-class training were randomly selected from the pool of respondents to the pre-training assessment and others were made aware of the program through traditional outreach efforts. 517 people were trained during 15 training sessions, with the last one finishing on August 27, 2021. Participants were students as well as professionals from industry and government institutions. In order to comply with COVID-19 safety protocols, participants were divided into two training rooms in order to not exceed 20 people per room.

Table 1 below shows that a vast majority of participants were male and this might result from a bias resulting from the recruitment method. More men are typically on Facebook than women in Kenya. Additionally, men might be drawn more intrinsically to the cybersecurity field than women. Achieving gender parity amongst participants was not a project requirement and would have required a different project design.

**Table 1: Summary Statistics of Participants**

| | **Total for grant** |
|---|---|
| # of training sessions | 15 |
| # of training participants | 517 |
| % men | 78% |
| % women | 22% |
| Average age | 25 |
| # of training evaluations received | 420 |
| Training evaluation score (maximum is 4) | 3.8 |
| Learning effect | 40% |

However, a key component of the project was to determine whether or not gender has any impact on knowledge and ability related to the cybersecurity field. In order to gain insights at the individual level, we used the 'partition around medoids' (PAM) algorithm to identify clusters of participants with similar characteristics.

There were 303 data points from people who completed both the pre and post training evaluations out of which we excluded participants who had average scores on the pre and post-training assessments. Without this exclusion, more distinct clustering patterns would not be visible. This process left 119 participants to be analyzed via PAM. Pre-training scores are shown on the x-axis whereas post-training scores are shown on the y-axis (see Chart 1).

The color-coded clusters shown in the chart are further identified in Table 2, which describes the characteristics of the clusters in more detail. The gender breakdown found in the PAM analysis (74% male and 26% female) is similar to the overall gender division of the trained cohort shown in Table 1 above.

**Chart 1: Clusters of Participants**

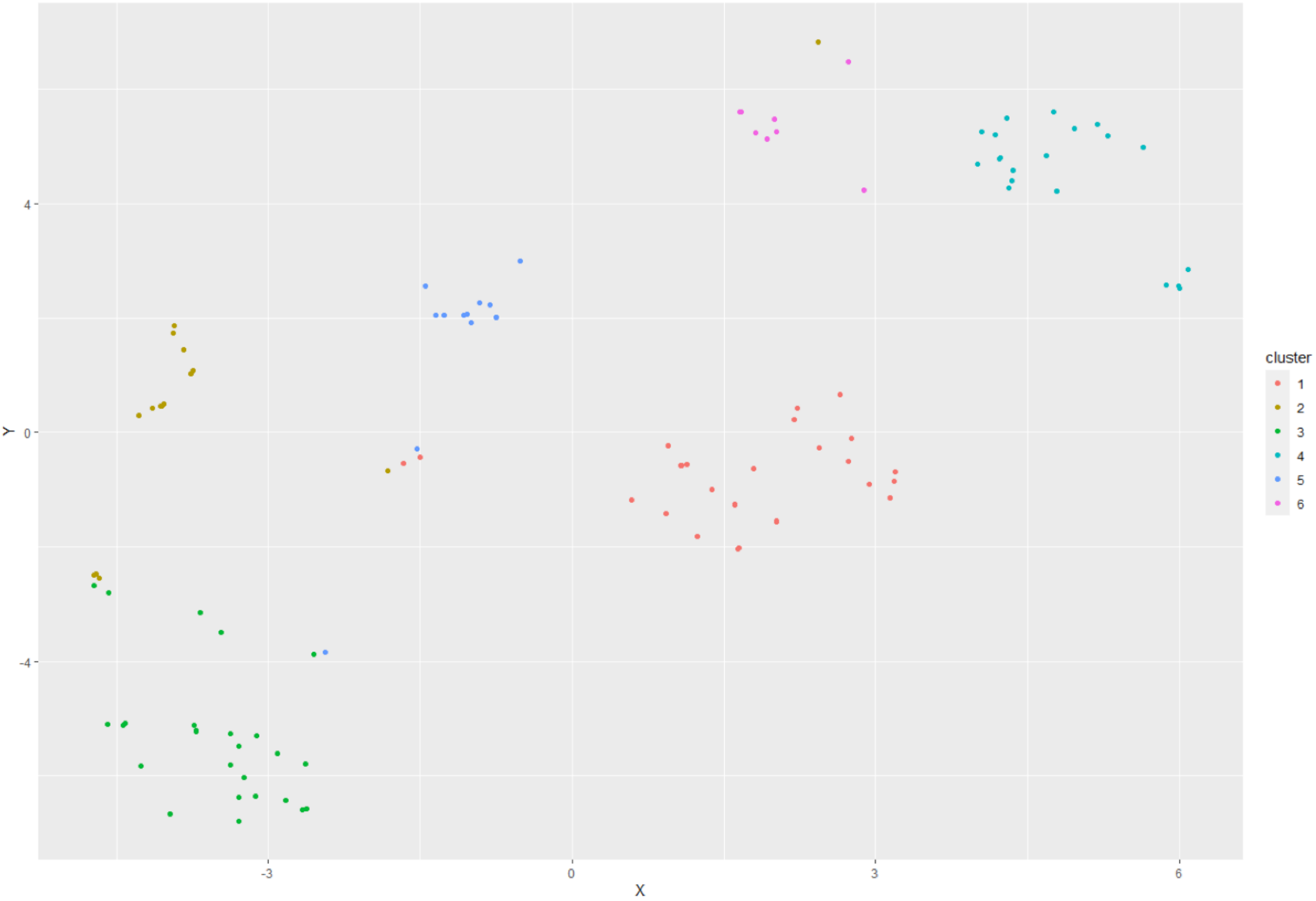

**Table 2: Summary Statistics of Clusters**

| **Criteria** | **Cluster 1** | **Cluster 2** | **Cluster 3** | **Cluster 4** | **Cluster 5** | **Cluster 6** |
|---|---|---|---|---|---|---|
| # of males | 31 | 18 | 27 | 0 | 12 | 0 |
| # of females | 0 | 1 | 0 | 23 | 0 | 7 |
| Mean pre-training assessment score | 7.1 | 6.1 | 7.5 | 7.2 | 7.7 | 7.1 |
| Mean post-training assessment score | 8.3 | 7.5 | 8.8 | 8.8 | 7.3 | 9.6 |
| Mean age | 24.6 | 22.2 | 24.9 | 23.1 | 27.0 | 26.3 |
| Graduate degree holders | 0 | 0 | 1 | 0 | 11 | 7 |
| Undergraduate degree holders | 30 | 0 | 22 | 21 | 0 | 0 |
| KCSE holders | 0 | 16 | 2 | 1 | 0 | 0 |
| Other education | 1 | 3 | 2 | 1 | 1 | 0 |
| # of people with previous cybersecurity training | 0 | 3 | 27 | 4 | 1 | 0 |

Observations from the cluster analysis are as follows:

- KCSE students performed disappointingly when looking at both the pre and post training evaluations (Cluster 2). This group was also the youngest;
- Cluster 3 consisted of only male students with undergraduate degrees and all had previous cybersecurity training. Despite their preexisting cybersecurity knowledge, their test scores were the lowest of all participants;
- Cluster 4 contained only females with undergraduate degrees and some had previous cybersecurity training. They exhibited a good learning effect, as shown by their test scores (it is almost identical to their male peers from cluster 1);
- Cluster 5 is a group of male students with graduate degrees who displayed poor performance in their post-training evaluations. This was the oldest group of students possibly indicating that they are working professionals;
- Cluster 6 is a group of female students with graduate degrees and no previous cybersecurity training. They scored the highest in the post-training evaluation and also showed the biggest learning effect.

## 5. Discussion of Findings

The project was designed with a rigorous monitoring, evaluation and learning plan in place. SRI was thus able to utilize a data driven approach to design the curriculum of the knowledge enhancement training and evaluate the project's outcome.

The training attracted participants with a variety of backgrounds and generally women performed as well as men in both the pre and post-training assessment (the exception being cluster 3). Particularly female students with graduate degrees were more willing to learn than their male counterparts although it is possible to be successful in the cybersecurity field by obtaining relevant skills trainings rather than higher degrees. **This means that more girls and women need to be encouraged to study STEM subjects and pursue professions in technology sectors.**

Most importantly, stereotypes about women in technology need to be critically examined and shattered. Given that the sector is well suited for skills enhancement through self-study, young women are just as competitive in the marketplace as men. This is particularly important when considering that while women attend university and TVETS at similar rates to men, they are far less likely to be formally employed. If employers use an aptitude based recruitment process, they will discover that formal education does not serve as a good predictor for on the job performance. Anybody with the right aptitude and training can be successful in the cybersecurity field.