Scientific
Research
Publishing

Closing the Cybersecurity Skill Gap in Kenya: Curriculum Interventions in Higher Education

Raphael M. Kaibiru[1], Simon M. Karume[2], Faith Kibas[2], Martin Luther Bwangah Onga'nyo[3]

[1]Machakos University, Machakos, Kenya
[2]Kabarak University, Nakuru, Kenya
[3]Unites States International University-Africa, Nairobi, Kenya
Email: rkaibiru90@gmail.com, smkarume@gmail.com, faykibas@gmail.com, onganyo1@gmail.com

Abstract

In the wake of increased cybercrime against insufficient cybersecurity professionals, there is an urgent need to bridge the skill-gap. The demand for skilled and experienced (approximately 40,000 to 50,000) cybersecurity professionals in Kenya is soaring all-time high. This demand is against the available 1700 certified professionals. Therefore, this paper seeks to bring to fore interventions put in place to address the skill gap through curriculum interventions. In order to get a clear understanding, the paper sought to determine the status of cybersecurity skill gap in Kenya and what universities are doing to address the gap. The paper also sought to propose the way forward to close the skill gap. This is a seminal review paper in the field of cybersecurity in Kenya focusing on institutions of higher learning and the interventions to address the cybersecurity skill gap. This research is significant to the general institutions of higher learning in both private and public universities. Results show that the cybersecurity skill gap is very high in Kenya. Interventions being offered by universities include partnerships with private cybersecurity organizations, offering cybersecurity certification training hackathons, and degree programs. However, it was established that only 13.2% of registered universities that offer cybersecurity degree programs in Kenya. The paper therefore strongly recommends launch of cybersecurity programs at the levels of undergraduate and graduate in many universities. This can therefore be augmented with other interventions such as certifications, hackathons and partnerships. Further research can be conducted to establish factors affecting the launch of cybersecurity programs in institutions of higher learning in Kenya. A further research can also be conducted to determine the effect of supplementary cybersecurity trainings such as hackathons and certifications.

Keywords

Cybersecurity, Cybersecurity Skill Gap, Cybersecurity Curriculum, Institutions

of Higher Learning

1. Introduction

The growth of Information technology (IT) has increased in the last decade in Africa. Most African countries have adopted IT with a clear understanding that IT is an enabler of business growth as well as an important tool for economic growth [1]. According to [2], the internet connectivity in Africa will contribute to $180 billion to Africa's economy by 2025 and a potential to reach $712 billion by 2050. To ensure these projections come to fruition, many African governments have created partnership with private and institutions of goodwill to connect over 700 million unconnected users to high-speed internet.

However, according to [3], connection without safety is meaningless due to the high rate of cybercrime incidents being reported in Africa. Owing to cybercrime, the GDP of Africa reduced by 10% to an estimated level of $4.12 billion in 2021 [3]. Several African countries have suffered serious cybercrime attacks. In the year 2020, South Africa recorded a series of cyber-attacks a 22% increase in 2019. According to [4] the cause of this spike was attributed to lack of investment in cyber security with a particular issue being the lack of skilled practitioners in the industry, poor public knowledge in threat landscape, lack of cybercrime legislations among others.

In Nigeria, cyber security is becoming a serious threat to the digital economy. A report by [5] indicates that mobile applications were a strong target for attackers. The report indicated that 576 malicious mobile applications were detected in the Google Play store. This is a serious problem based on the fact that there was an increase in adoption of mobile devices and overreliance on mobile money transactions. The case was not better in Ethiopia either. [6] reported that attacks doubled in the year ending 2020/2021. The number had increased from 1080 to 2800 cases in the year 2021.

Cases of cyber insecurity are being reported in East Africa as indicated in a report by [7] that East African countries were highly affected by cyberattacks. According to the report, 31% of organizations reported that they had fallen victim of cyberattacks. This translates into the highest number in Africa.

Kenya is one of the many countries in Africa that has continued to grow in information Technology adoption. This has been made possible by governments support and efforts to accept the entry of high speed undersea fiber cable [8]. The internet penetration coupled with increased adoption of mobile technology has given an impetus to the growth of digital economy in Kenya. Many businesses, governments and organizations have established beneficial collaborations which have created a big appetite for the valuable information stored in the information systems used. Cybercrime has become one of the major issues affecting the smooth and comfortable use of Information technology in Kenya [1] [8].

With the growing cybercrime reports from both academic research, business analyst reports and conference seminars state that there is a growth in cybersecurity skill gap as the continent of Africa and the world information technology adoption grows [9]-[14]. According to [12] report on the skill gap in cyber security in Africa, there were 1700 skilled cyber security professionals in Kenya. The report projected a 60% skill gap shortage in most organization in the year 2019.

The growing cybercrime coupled with the ever-widening gap between the available skilled labor and the market demand has triggered policy maker and governments to propose workable solutions [1] [15]. In Kenya, the government has in the recent years implemented strategies, laws, policies and formed constitutional bodies and institutions to address cybersecurity concerns in the country [1] [8] [9] [10] [12].

According to the cybersecurity strategy of Kenya the government of Kenya is working towards capacity building by encouraging institutions of higher learning to have curricula that are aimed at training competent cybersecurity professionals [16].

Despite these brilliant interventions suggested by experts and governments, statistics on cybercrime continue to bedevil the digital cyber space in Kenya. In the year 2017 according to [17] Kenya was reported to have lost Shillings 21.2 billion to cyberattacks. These statistics placed Kenya second where Nigeria lost Shillings 65.5 billion.

With the ever-growing cybersecurity issues one of the main pain points in addressing the matter is the lack of skilled manpower. According to [18] as shown in **Figure 1** and **Figure 2**, it is more difficult to a attract people with cybersecurity skills by employers.

This paper seeks to bring into perspectives intervention offered by institutions of higher learning to close the cybersecurity skill gap in Kenya.
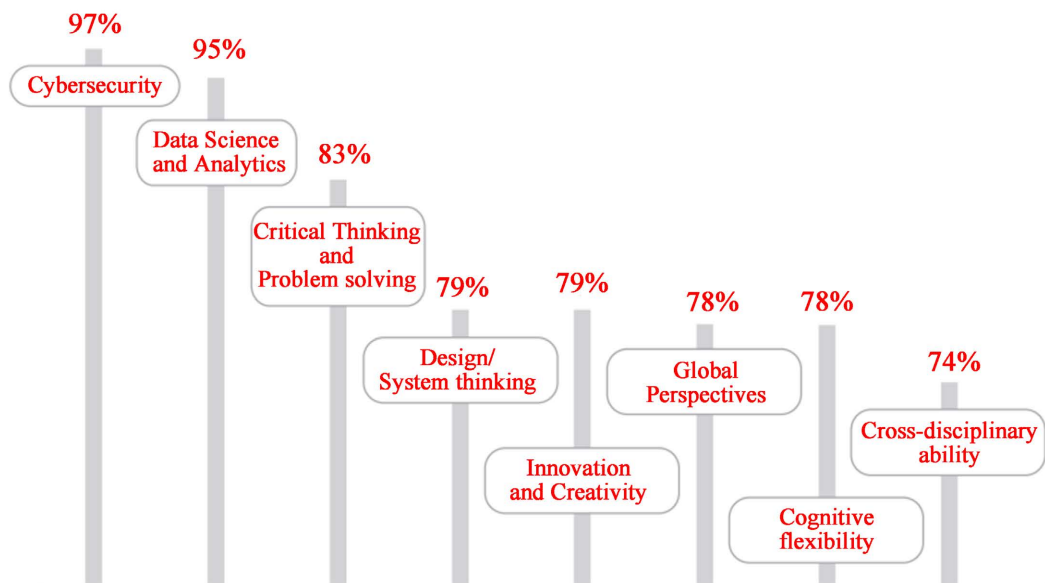

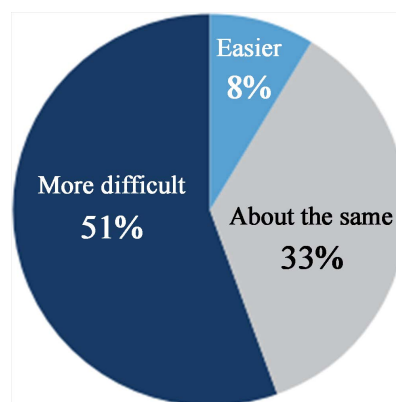**Figure 1.** Difficulty of finding Cybersecurity Skills [18].

Figure 2. The ease of finding people with Cybersecurity skills [18].

2. Problem Statement

Kenya is banking on Information Technology to spur economic growth as envisioned in the Vision 2030. The government of Kenya has recognized the need for a skilled cybersecurity labor in the wake of increased cybercrime. Cybercrime cases are a major threat to achievement of a successful and stable digital economy. As it was identified by [1] [12] [13] lack of skilled, competent and experienced human capital is one of the contributing factor to the high rate of cybercrime. This is despite the fact that the government of Kenya has made a requirement to education institutions to develop curricula to address the ever-growing skill gap [16]. This research is significant to both the public and private institutions of higher learning, which will help to determine some of the interventions that can be applied to address the cybersecurity skill gap.

3. Study Objective

The aim of this study is to determine measures taken by institutions of higher learning to address the cybersecurity skills gap in Kenya.

Specific Objectives

This paper sought to address the following objectives.

1) To determine the status of cybersecurity skill gap in Kenya.

2) To determine cyber security interventions by institutions of higher learning in Kenya.

3) To recommend the way forward with regard to closing the skill gap in cybersecurity in Kenya.

4. Research Methodology

An integrative review research approach was adopted in this study. To identify relevant papers in cyber security skills gap in Kenya, a traditional search method was adopted using key words "cybersecurity skill gap in Kenya". Only papers with key terms cybersecurity skill gap in Kenya were selected for review in this study. Secondary data regarding cybersecurity related programs offered in uni-

versities in Kenya was collected by visiting the website of both private and public universities. According to the Kenya Universities and College Central Placement Service (KUCCPS) website, there are 68 registered public and private chartered universities. KUCCPS is a government organization under the ministry of education that is mandated to place students in various academic programs offered in the institutions of higher learning. Therefore, the data collected is original and authentic for this research. The researcher viewed all the programs offered by each of the registered university to identify those that are offering programs in cybersecurity, audit and forensics.

The review was aimed at determining the current status of cybersecurity skill gap in Kenya, the interventions put in place by universities and the way forward to enable close the ever-widening gaps.

5. Literature Review

5.1. The Status of Cybersecurity Skill Gap in Kenya

This section provides an examination of the status of cybersecurity skill gap in Kenya. Kenya continues to face increased cyberattacks. Several studies have linked this problem to the growing demand and low supply of skilled cybersecurity professionals.

Before getting into the details of cybersecurity skill gap in Kenya, it is worth providing a definition of the term skill-gap. According to [19] skill gap is the significant gap between the capabilities of the organization and the skills available to help the organization achieve its goals. Another definition by [20] states that skill gap is the phenomenon whereby the skill levels of the available workers are insufficient to address the needs of the current job. Going by these two definitions then it is sufficing to state that cybersecurity skill gap is the gap between the available skills in cybersecurity and the work that needs to be done in a particular organization.

The widening gap between the available skilled workers and the demand is growing at an alarming rate. According to the cybersecurity workforce study [21] the global demand for skilled workers doubled despite an increase of the same in the previous year. This challenge is being felt in many countries especially in developing countries like Kenya.

The cost of cybercrime in Kenya has been on the rise over the years as indicated in the annual cybersecurity reports by cybersecurity research farm Serianu. According to the cybersecurity report [22] estimated that cybercrime had a financial loss of $175 Million. In the same report it was indicated that there were only 1400 certified cybersecurity professionals. This was an increase from,000 certified professionals that were reported in the previous year. This grim statistics on the status of cybercrime costs soared higher in the year 2018 with a record of $295 Million (Serianu, 2018). The ever-growing cases of cyber crime coupled with myriad of challenges among them insufficient number of skilled cybersecurity professionals has led to the high cost of financial loss in the GDP

of Kenya.

According to a report by [23] looking at the cybersecurity skill gap in Kenya, it was noted that there were only 1700 certified professionals in Kenya as shown in Figure 3. It was also noted that companies were faced with a challenge of hiring professionals because of lack of experience as well as high renumeration rate requested by the available experts. The report also indicated that the gap would grow by 60% in the year 2019. This finding is in support of what was reported by [24] that there was lack of skilled technical cybersecurity professionals in Africa.

As reported by [25] the ever-widening cybersecurity skill gap was likely to reach 40,000 if it remained unaddressed. This statistic is in line with what was projected that Kenya would be in need of 50,000 professional by the year 2023 [23].

Kenyan organizations are facing challenges when hiring cybersecurity professionals. When responding to the question of challenges faced when hiring professionals, managers cited lack of experience and high remuneration expectations as the main challenges as shown in Figure 4.

This increasing demand against the available manpower is calling for an urgent intervention. Several proposals have been fronted with the main solution being technical hands-on training for professionals in cybersecurity in Kenya. Much of the interventions has been implemented through partnerships between private organizations and universities as well as other complementary training colleges [25] [26] [27] [28].

During the launch of Cyber Shujaa program at United States International University-Africa (USIU-Africa) [26] the Vice Chancellor noted that gap and shortage of cyber skills was continuing to grow and this was impacting on professionals hence making them feel unprepared for various attacks.
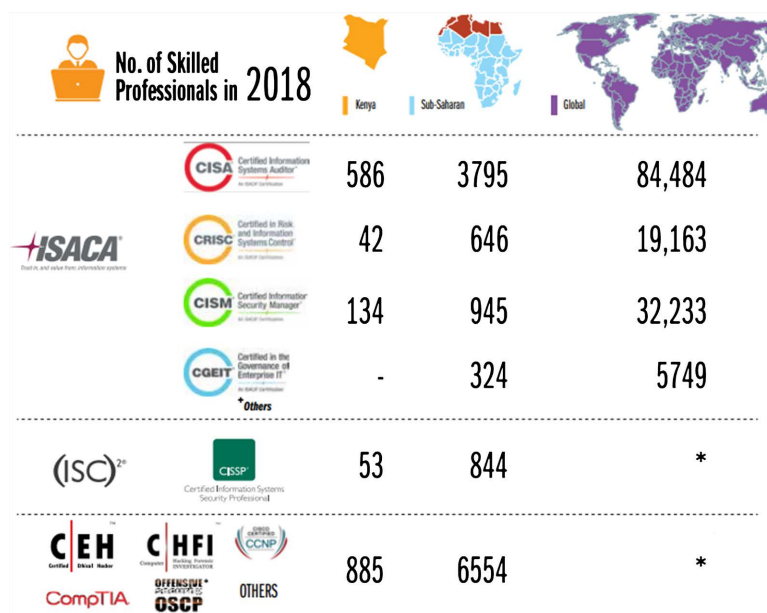

No. of Skilled Professionals in 2018		Kenya	Sub-Saharan	Global
ISACA	CISA — Certified Information Systems Auditor	586	3795	84,484
	CRISC — Certified in Risk and Information Systems Control	42	646	19,163
	CISM — Certified Information Security Manager	134	945	32,233
	CGEIT — Certified in the Governance of Enterprise IT *Others	-	324	5749
(ISC)²	CISSP — Certified Information Systems Security Professional	53	844	*
CEH CHFI CCNP CompTIA OSCP OTHERS		885	6554	*

Figure 3. Number of certified cybersecurity professionals in Kenya [23].
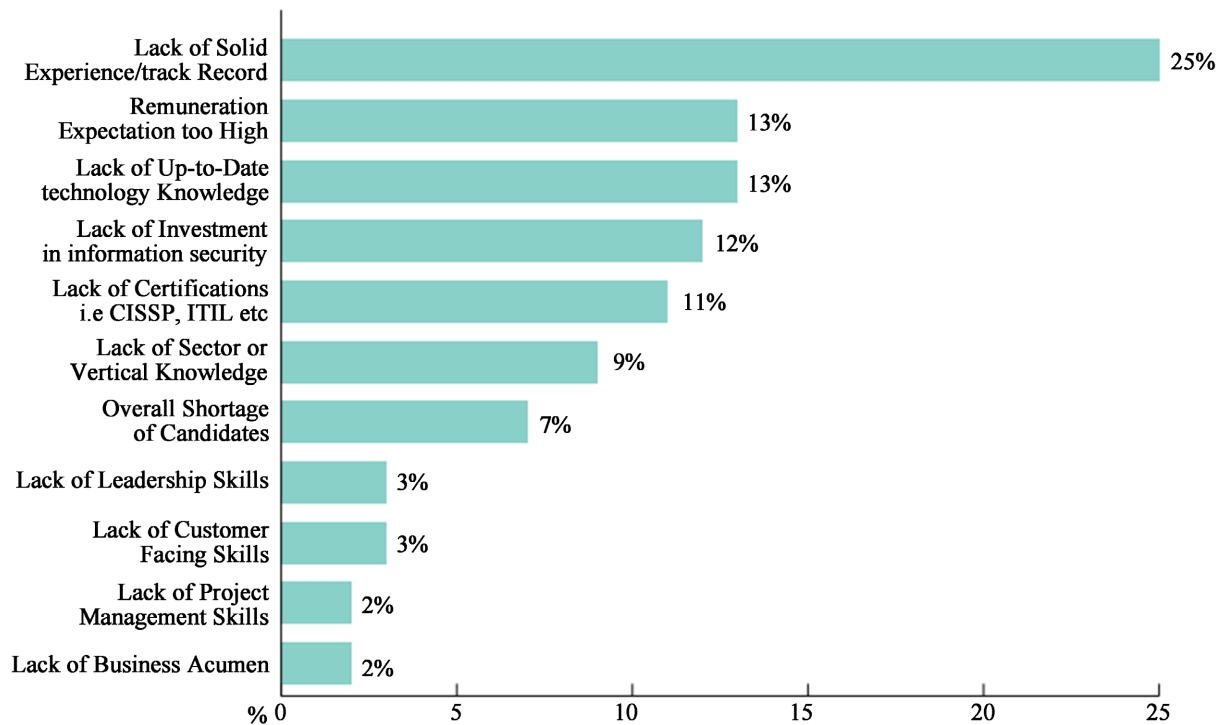
Figure 4. Constraints when hiring cybersecurity professionals [23].

The following section provides a discussion of interventions undertaken by universities to address the cybersecurity skill gap in Kenya.

5.2. Interventions for Cybersecurity Skill Gap in Kenya: What Are Universities Doing about It?

This section examines interventions undertaken by universities in Kenya with regard to addressing cybersecurity skill gap. The main aim will be to identify whether there are cybersecurity academic programs being offered in institutions of higher learning in Kenya.

The interventions will be categorized into three. Intervention through partnerships with cybersecurity private organizations, cybersecurity Hackathons and independent or inhouse cybersecurity curriculum development.

5.2.1. Intervention through Partnerships with Private Organizations

So far it is clear from the previous section that insufficient cybersecurity manpower is a real problem. Businesses, organizations, governments and individuals are being affected by the global shortage of skilled cybersecurity manpower. As a result, cybersecurity companies have found it necessary to plug the gap by partnering with universities and colleges to train market-ready and skilled manpower. As noted by [29] cybersecurity is no longer a boring technology story that we can ignore and treat as an afterthought.

According to [30] [31] [32] collaboration between private organizations and higher education institutions can play a pivotal role in addressing skill gap in cybersecurity. Such collaborations are very beneficial to students, institutions of

higher learning and private organizations. According to [32] partnerships between higher education and private organizations ensure students graduates come out equipped with skills on threat landscape and how to counter them.

In addition, [30] noted that such partnerships also have a benefits to both the institutions of higher learning and private organization. Universities benefit by developing strong reputation for graduates with market ready skills, high enrolment rate and direct benefits from resources invested in their institutions such as software, hardware, grants and also technical expertise. To the private organizations, benefits come from transferring cybersecurity skills into the classroom, which gives them time and resources to focus on developing skills specific to the organization. By developing cybersecurity curriculum, private organizations influence skills learnt by cybersecurity professionals other than their own employees, which makes it easier to hire cybersecurity experts in future.

In Kenya partnership has been the quickest approach to addressing the problem, whereby many organizations have partnered with both public and private universities. This approach is proposed in the National Cybersecurity Strategy report of 2014 in addition to curriculum development by universities [16]. The following section is discussion of some examples of university and private partnerships in Kenya.

University of Nairobi C4DLab in Partnership with ICT Authority

As a measure to address the ever-growing gap between the available skills and what the employer wants, university of Nairobi through the assistance of ICT Authority of Kenya started a cybersecurity program. According to [33] the program is aimed at addressing the capacity deficit in the industry. Despite this intervention, the program was targeting government employees as well as private business employees. The target audience was individuals with a background in computer science, risk management, forensics, cloud application developers among others.

Partnership between Strathmore University and Fortinet Security Academy

According to [34] Strathmore University entered into a collaborative partnership with Fortinet a global leader in cybersecurity solutions to offer cybersecurity training to students in order to close the skill-gap in the Kenyan meeting.

This partnership was necessitated by the growing demand for employees with cybersecurity skills in Kenya. This collaboration was aimed at giving the university an edge to leverage on its cybersecurity curriculum. During the launch it was noted that Strathmore was the first university in Kenya to join Fortinet Security Program.

Partnership between United States International University-Africa, Kenya Bankers Association and Serianu

In the last six-year Serianu, Kenya Bankers Association (KBA) and United States International University-Africa (USIU-Africa) have been conducting research to understand the gaps within ICT and cybersecurity in Kenya and Africa. According to [35] results from the study indicated that there were three chal-

lenges namely job placement gap-that every year 1,000,000 youths join the labor market and majority of them go unemployed, skills mismatch challenge—that there was a skill mismatch between what youths are taught in school and what the industry wants and gender inclusion-whereby there were few women especially in the cybersecurity profession.

From these three challenges, a multisectoral partnership launched a training and placement program dubbed "Cyber Shujaa" to train 2000 youth in cybersecurity in three years. To address the gender deficit, the program aims to train 1000 women, who will make up 50% of the total target number. The program according to [35] aims at providing practical curriculum, vigorous training, placement into organizations and mentorship.

It was noted that KBA would provide market intelligence that would inform curriculum development, USIU-Africa would develop the curriculum while Serianu would provide practical training.

During the graduation ceremony of the first and second cohort of cybersecurity experts graduates, it was noted that 170 trainees graduated from Cyber Shujaa program. However, 90 of these trainees were employees selected from 47 banks in Kenya. This is an indication that the partnership is skewed towards filling the cybersecurity skill gaps in banking sector.

5.2.2. Partnership with Cybersecurity Certification Academies

Professional certification in cybersecurity is regarded as must have to determine hands-on skills when hiring for cybersecurity roles. According to [30] [31] [36] most manager consider cybersecurity professional certification when hiring for a cybersecurity role. As noted [30] that despite requiring a candidate to possess a bachelor's degree in cybersecurity, managers rank hands-on experience and certification as better methods of acquiring cybersecurity skills than earning a four year degree.

These sentiments are supported by [37] [38] who states that professional certification give the holder benefits in showcasing their knowledge and expertise alongside your industry experience, increases employability and it also adds to the ethical character.

However, acquiring cybersecurity certification as a measure of cybersecurity skills among professionals has been challenged. According to [30] although most job posting emphasize on certification, many employers have disabused this notion indicating that certification is necessary but not sufficient when making decisions to hire a cybersecurity professionals. This is because there exists a gap between certification and hands-on skills coupled with real-world problems.

Universities Offering Cybersecurity Professional Certificate in Kenya

In addressing the cybersecurity skill gap higher education institutes in Kenya establish partnerships with international certification bodies. According to [39] there are three universities Strathmore University, United States International University Africa, KCA University and KeMU University that offer Certified Ethical Hacking (CEH). Certified Ethical Hacking certification is one of the worlds

sought after qualification when hiring a cybersecurity professional.

Others offer security certification training as a component within a domain specific training such as Networking security. According to [40] website, there is an ICT training center for certified professionals in various domains including cybersecurity. Some of the certification partners include Huawei Academy, IBM Skills Academy, Cisco Networking Academy and ICDL Center.

5.2.3. Interventions through Cybersecurity Hackathons

Another method being applied to address the cybersecurity skill gap is use of a concept called "Hackathon". According to [41] [42] hackathon is a name from two terms hacking and marathon, which means an activity that involves intense and uninterrupted programming to solve a problem or come up with a new innovation.

Cybersecurity hackathon is an intense process in which cybersecurity enthusiast meet to try and break into computer codes as well as provide a solution to the identified weakness. Hackathons are either organized by organizations, institutions of higher learning or a collaboration between universities and private organizations.

According to [30] exposing cybersecurity students to bootcamps gives them opportunity to develop practical skills and experience which can be of help when applying for cybersecurity positions.

In Kenya, cybersecurity hackathons have gained momentum especially with universities. Students from various universities attend these hackathons to showcase their skills in security. The following is a discussion of cybersecurity hackathons organized between universities and organizations in Kenya.

Communication Authority Security Hackathon

Communications Authority of Kenya is one of the organizations that hosted a cybersecurity hackathon in Kenya. According to [43] the hackathon featured various universities in in which students were to compete in various categories. In this particular hackathon, students were required to apply their hacking skills to solve computer security problems. The event was aimed at showcasing the technical skills that are required to address the problem facing the country.

In October 2022 three companies partnered to organize a second Cybersecurity Hackathon. These companies are Huawei, Communications Authority of Kenya (CAK) and Kenya Cybersecurity and Forensics Associations (KCSFA). The competition brought together over 100 students from universities in Kenya [44]. The competition ended by rewarding three teams that emerged winners out of the twenty-four groups that had participated.

5.3. Intervention through Cybersecurity Curriculum

5.3.1. The Need for Cybersecurity Programs

Institutions of higher learning play a pivotal role in developing programs that address professional market gaps. As digitization continues to gain momentum in adoption and computer crimes being reported more-often, the demand for

trained and skilled labor grows. Therefore, there is need for universities to launch cybersecurity programs at various levels-diploma, bachelor's and graduate. This is because according to [45] traditional computer science programs do not educate students to acquire skills in cybersecurity. With many universities offering computer science programs, [45] suggests that there is need for a development of curricula that addresses in particular cybersecurity.

According to [46] [47] the demand for cybersecurity professionals with a bachelor's degree was high compared to other levels, with 78% and 65% as shown in Figure 5 and Figure 6 respectively for the year 2014 and 2019. Also according to [18] 61% of the respondents said that it was necessary for undergraduate students to be taught cybersecurity skills in university program.

These reports finding communicates to universities that there is a need to develop curricula in cybersecurity with a main focus on bachelor's degree followed by master's program.
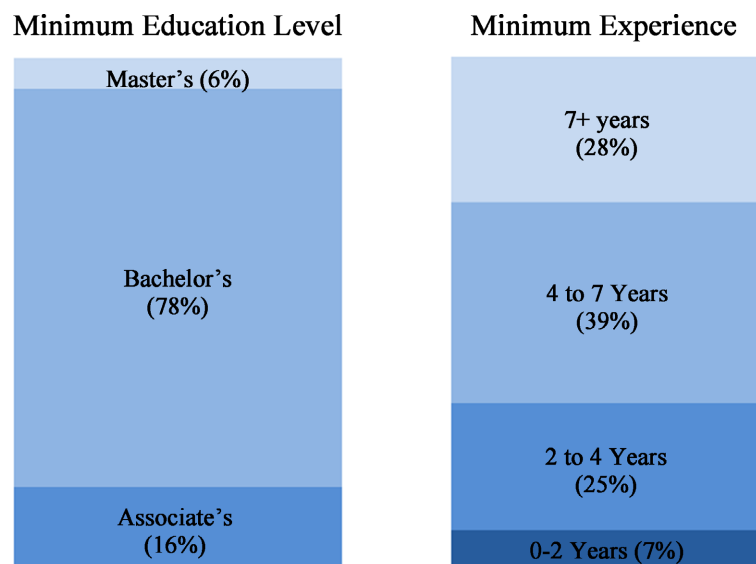

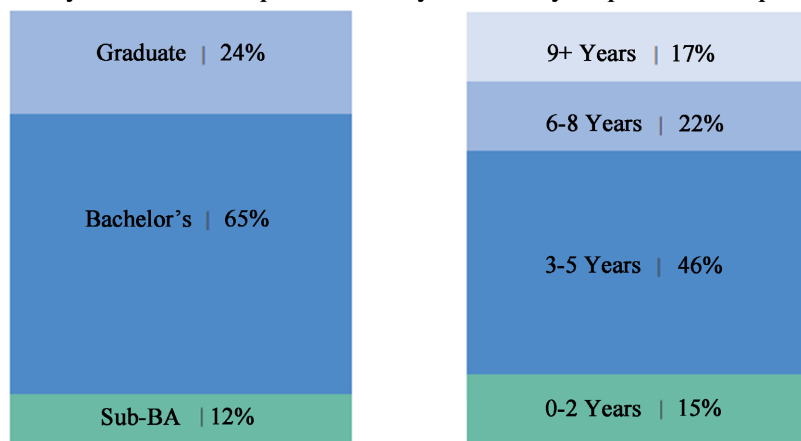Figure 5. Minimum education requirements 2014 [46].

Figure 6. Minimum education level 2019 [47].

5.3.2. Cybersecurity Degree Programs in Universities in Kenya

This section sought to establish whether universities in Kenya offer programs in cybersecurity. According to [16] universities are required to develop curricula to train students in the profession of cybersecurity to address the every growing concern of cybercrimes in the country.

According to the data from Kenya Universities and College Central Placement Services (KUCCPS) website there are 68 registered universities on the portal together with 121 colleges which offer approximately 990 accredited programs. A desktop survey from the 68 registered universities found that 9 out of the registered universities offer training in computer security, information system security and audit, cybersecurity and forensics. This translates to 13.2% of the total registered universities. Table 1 shows the distribution of these universities with the respective program levels.

It is clear that most of the sampled universities in Kenya offer undergraduate programs in computer security related subject. This is in line with what was reported by [18] [30] [46] that most employers consider undergraduate programs necessary to impart cybersecurity skills.

6. The Way Forward for Kenyan Universities

The world is facing an ever-growing problem with cybercrime as more and more computing devices join the internet. The growing demand for skilled cybersecurity manpower increases the supply should be provided. There are several interventions that can be applied to address this problem such as partnerships with private organizations, participation in hackathons for industry experience, certification training and curriculum development [30] [31] [32] [41] [42] [46].

However, since this paper was focusing on curriculum interventions, curriculum development for undergraduate programs in cybersecurity should be adopted by many institutions of higher learning in Kenya. As it was noted in Table 1,

Table 1. Cybersecurity programs offered in universities in Kenya.

No.	University	Program Level			
		Diploma	Bachelor's	Master's	PhD
1	Cooperative University		1		
2	Kabarak University		2	1	1
3	JOOUST	1	2	1	1
4	Masinde Muliro University			1	
5	Meru University		1		
6	KCA University		1		
7	Riara University	1			
8	Machakos University		1		
9	Strathmore University			2	

147

13.2% of the sampled universities offering cybersecurity related programs, is a small number to produce the required skilled labor in the demanding market. Therefore, as noted by [18] [30] [45] [47] there is need to start training undergraduate students in cybersecurity skills. However, [22] [25] notes that there is need for one to acquire a cybersecurity certification to demonstrate the skills as many fresh graduates lack the needed skills to tackle the security problems effectively.

7. Conclusions

Despite the increasing demand for cybersecurity skills amidst high cybercrime rates, interventions adopted by institutions of higher learning in Kenya are encouraging. The adoption of private partnerships, introduction of hackathons, certifications and development of academic curricula is a positive indicator of the will and commitment towards addressing the skills gap.

The 13.2% of universities offering computer security related programs can be termed as the journey of a thousand miles which begins with one step. Realistically, this is not enough to meet the 50,000 professional demands projected by [23]. Therefore, more universities should be encouraged to implement curricula in both undergraduate and graduate levels as noted by [30] [46]. Among other interventions, this can be used as a base catalyst to spur the growth and adoption of cybersecurity skills in the country as well as the continent. Further research can be conducted to establish factors affecting the launch of cybersecurity programs in institutions of higher learning in Kenya. A further research can also be conducted to determine the effect of supplementary cybersecurity trainings such as hackathons and certifications.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1]   Symantec (2016) Cyber Crime and Cybersecurity Trends in Africa.

[2]   IFC & Google (2020) Economy Africa 2020: Africa's $180 Billion Internet Economy Future.

[3]   Adegoke, A., Boakye, B. and Garson, M. (2022) Cybersecurity in Africa: What Should African Leaders Do to Strengthen Teh Digital Economy? Tony Balir Institute for Global Change.
https://institute.global/policy/how-rethink-cybersecurity-africa-strengthen-digital-economy

[4]   Accenture (2020) Insights into the Cyberthreat Landscape in South Africa.

[5]   Okeowo, Y. (2021) Mobile Malware Epidemic Hits Nigeria; 1 in 9 Android Phones Now Infected.

[6]   Xinhua (2021) Cyber Attack Attempts More than Double in Ethiopia This Year.
https://africa.cgtn.com/2021/09/07/cyber-attack-attempts-more-than-double-in-ethiopia-this-year

[7] KPMG (2022) Africa Cybersecurity Outlook.

[8] Ndenda, A. and Collins, O. (2019) Cyber Threats and Cybersecurity in Kenyan Business Context. *Global Scientific Journal*, **7**, 576-582.

[9] Kagwiria, C. (2020) Cybersecuirty Skills Gap in Africa. AFRALTI.
https://www.afralti.org/cybersecurity-skills-gap-in-africa

[10] Mwenda, E. (2022) Demand for Cybersecurity Experts Grows on Attacks. *Business Daily*.

[11] Waithaka, S. (2016) Factors Affecting Cyber Security in National Government Ministries in Kenya. University of Nairobi, Nairobi.

[12] Serianu (2018) Kenya Cybersecurity Report 2018.

[13] Kanali, N. (2022) New Cyber Hujaa Program Bridges Country's Cybersecurity Skills. African Business Community.

[14] Gitahiga, G., Kapiyo, V., Kivuva, M., *et al.* (2022) A Study Paper on Human-Centred Cybersecurity: Kenyan Fintech Sector.

[15] Kshetri, N. (2019) Cybercrime and Cybersecurity in Africa. *Journal of Global Information Technology Management*, **22**, 77-81.
https://doi.org/10.1080/1097198X.2019.1603527

[16] Government of Kenya (2014) National Cybersecurity Strategy 2014. Ministry of Information and Communication Technology.

[17] Serianu (2017) Demystifying Africa's Cybersecurity Poverty Line.

[18] BHEF (2017) Understanding Cybersecurity Talent Needs Findings from Surveys of Business Executives and College Presidents. GULLUP.
https://www.bhef.com/sites/default/files/bhef_2017_cybersecurity.pdf

[19] ASTD (2012) Bridging the Skill Gap: Help Wanted, Skills Lacking: Why the Mismatch in Today's Economy?

[20] Seamus, M. and Luis, O. (2015) Skill Gaps in the Workplace: Measurement, Determinants and Impacts. EconStor.
https://www.econstor.eu/bitstream/10419/114146/1/dp9278.pdf

[21] (ISC)2 (2022) A Critical Need for Cybersecurity Professionals Persists amidst a Year of Cultural and Workplace Evolution. (ISC)2 Cybersecurity Workforce Study.

[22] Serianu (2016) Achieving Cyber Security Resilience: Enhancing Visibility and Increasing Awareness. Serianu, Kenya Cyber Security Report 2016.

[23] Serianu (2018) Cyber Security Skills Gap. Serianu, Kenya.
https://www.serianu.com/downloads/KenyaCyberSecurityReport2018.pdf

[24] Seck, M., Belai, T. and Nwuke, K. (2014) Tackling the Challenges of Cybersecurity in Africa. United Nation Economic Commission for Africa.
https://repository.uneca.org/bitstream/handle/10855/22544/b11079411.pdf?sequence=1&isAllowed=y

[25] EC-Council (2018) EC-Council and Extant Group Work toward Reducing the Huge Talent Gap in the Kenyan Cybersecurity Industry, Which Threatens to Exceed 40,000 Professionals.
https://www.eccouncil.org/ec-council-and-extant-group-work-toward-reducing-the-huge-talent-gap-in-the-kenyan-cybersecurity-industry-which-threatens-to-exceed-40000-professionals

[26] Aptantech (2022) Cyber Shujaa Program Aims to Bridge Kenya's IT Security Skills Gap.
https://aptantech.com/2022/07/29/cyber-shujaa-program-aims-to-bridge-kenyas-it-security-skills-gap

[27] Capital Business (2020) Strathmore University to Address Cybersecurity Skills Gap Following New Collaboration.
https://www.capitalfm.co.ke/business/2020/07/strathmore-university-to-address-cybersecurity-skills-gap-following-new-collaboration/

[28] KBC (2022) Women in Cyber Security|Stanchart Launch Mentorship Program.
https://www.kbc.co.ke/women-in-cyber-security-stanchart-launch-mentorship-program/

[29] Mukiibi, H. (2019) Cyber Security in Africa: The Boring Technology Story That Matters. *XRDS*: *Crossroads*, *The ACM Magazine for Students*, **26**, 56-59.
https://doi.org/10.1145/3368077

[30] BHEF (2017) Invest to Improve the Cyber Security Talent Deficit. Business Higher Education Forum. https://files.eric.ed.gov/fulltext/ED580862.pdf

[31] Moore, M. (2022) Cybersecurity Hiring: Why Employer and Higher Ed Collaboration Is Key. INFOSEC.
https://resources.infosecinstitute.com/topic/cybersecurity-hiring-why-employer-and-higher-ed-collaboration-is-key/

[32] Zurkus, K. (2018) How Can Industry Leaders and Academia Help Improve Cybersecurity Education? Security Intelligence.
https://securityintelligence.com/how-can-industry-leaders-and-academia-help-improve-cybersecurity-education/

[33] C4DLab (2022) Cybersecurity Training.
http://c4dlab.uonbi.ac.ke/training/cybersecurity/

[34] SmartInvestor (2020) Strathmore University Joins Fortinet Security Academy to Tackle Cybersecurity Skills Gap in Kenya. SmartInvestor.
https://smartinvestor.co.ke/4315/strathmore-university-joins-fortinet-security-academy-to-tackle-cybersecurity-skills-gap-in-kenya/

[35] USIU-Africa (2022) Launch of the CyberShujaa Program.
https://www.usiu.ac.ke/2541/launch-cybershujaa-program/

[36] Serianu (2017) Demystifying Africa's Cyber Security Poverty Line. Serianu, Kenya Cyber Security Report 2017.

[37] Chad, K. (2018) The Benefits of Cybersecurity Certifications. SBS Cybersecurity.
https://sbscyber.com/resources/the-benefits-of-cybersecurity-certifications

[38] Zorz, M. (2019) Exploring the Benefits of Cybersecurity Certification. HelpNetSecurity. https://www.helpnetsecurity.com/2019/10/29/cybersecurity-certification/

[39] Kenyaplex (2022) Colleges and Universities Offering Certified Ethical Hacker (CEH) in Kenya.
https://www.kenyaplex.com/courses/3576-certified-ethical-hacker-ceh.aspx

[40] Kenyatta University (2022) ICT Professional Training and Certification Center (IPTCC). http://ku.ac.ke/cisco/

[41] Komssi, M., Pichlis, D. and Raatikainen, K. (2015) What Are Hackathons for? *IEEE Software*, **32**, 60-67. https://doi.org/10.1109/MS.2014.78

[42] Uffreduzzi, M., Pellizzoni, E. and Dell, C. (2017) Hackathon as Emerging Innovation Practice: Exploring Opportunities and Challenges through 8 In-Depth Case Studies. Politecnico Milano 1863.
https://www.politesi.polimi.it/bitstream/10589/137237/5/Hackathon%20as%20Emerging%20Innovation%20Practice.pdf

[43] Abuya, K. (2019) Strathmore and UoN Top Cybersecurity Hackathon Hosted by the Communications Authority. Techweez.

https://techweez.com/2019/10/28/communications-authority-hackathon-nairobi/

[44] Opera, N. (2022) Cybersecurity Awareness Month: Kenya on Good Track on Matters of Cyber Attacks Prevention. Opera News.
https://ke.opera.news/ke/en/digital-technology/6e09224cc1ead9dadaef5e6c0a3b0555

[45] Crumpler, W. and Lewis, J. (2019) The Cybersecurity Workforce Gap. Center for Strategic and International Studies, Washington DC.
https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/190129_Crumpler_Cybersecurity_FINAL.pdf

[46] Burning Glass Technologies (2014) Job Market Intelligence: Report on the Growth of Cybersecurity Jobs. Burning Glass Technologies.

[47] Burning Glass Technologies (2019) Recruiting Watchers for the Virtual Walls: The State of Cybersecurity Hiring. Burning Glass Technologies.