Cybersecurity Capability and Capacity Building for South Africa

Joey Jansen van Vuuren, Louise Leenen

Cybersecurity Capability and Capacity Building for South Africa

Joey Jansen van Vuuren[1] and Louise Leenen[2]

[1] Tshwane University of Technology, Pretoria, South Africa
[2] Council for Scientific and Industrial Research, Pretoria, South Africa
lleenen@csir.co.za

Abstract. Cybersecurity capability and innovation cannot be attained by a single party; researchers, government, private industry and academia should join hands and create public-private partnerships to share their knowledge and create solutions. If South Africa wants to be sufficiently equipped to respond to cyber-threats and to ensure growth in the cybersecurity sector, the country needs to strengthen the pipeline of cyber talent and support the development of a cybersecurity workforce. These requirements provide an opportunity for industry, in collaboration with government and academia, to initiate innovative and exciting approaches to establish cybersecurity and a cybersecurity workforce in South Africa. This paper considers measures for governments, business and academia to alleviate the cyber skills shortage, and pay particular attention to the South African case.

Keywords: Cybersecurity Workforce, Cybersecurity Training, Cybersecurity Skills Shortage.

1 Introduction

A secure cybersecurity environment requires a robust workforce [1]. The current shortage of cybersecurity capability is a worldwide phenomenon resulting in companies and citizens being vulnerable to cyber-threats due to a lack of cybersecurity skills. Cybersecurity attacks are an inevitability [2] and the increasingly complicated threats that change on a daily basis, result in an inability of the insufficient number of qualified cybersecurity professionals to maintain security [3]. Christos Dimitriadis, Systems Audit and Control Association (ISACA) board chair and group director of Information Security for INTRALOT, confirms that due to the increase in cyber-attacks, enterprises need more resources to protect data and are facing a challenge in finding top-flight security practitioners with the necessary skills to do the job [2]. Jim Michaud, director of Human Resources and Business Development at the SysAdmin, Audit, Networking, Security (SANS) Institute, already emphasised this fact in 2015 by stating "Cybersecurity is the single most important business issue for so many CIOs right now, and the situation is going to get worse before it gets better" [4]. The 2015 Global Cybersecurity Status report, published by ISACA in 2015, indicated that there were already 300 000 unfilled cybersecurity jobs in the US alone and estimated this figure would increase to

1.5 million by 2020 [4]. According to the US Bureau of Labor Statistics, the demand for cybersecurity professionals will grow by 53 % during 2018. Industry, governments, academia and non-profit organisations need to work together and focus aggressively on meeting this need [3]. Speculation is that the market for cybersecurity professionals may be growing 12 times faster than the U.S. job market as a whole [5] .

The broad scope of the cybersecurity includes policies, standards that requires compliance from the perspective of software engineering and application security, and this is also a contributing factor to the skills shortage as indicated by Jenn Henley, Director of Security for Facebook. [6]. South Africa is still in their infancy in this process; although the National Cybersecurity Policy (NCPF) was approved in 2012 very few of the regulatory frameworks are in place. Cybersecurity education in the country is mostly limited to short courses or specialisation modules in a Masters Degrees.

2 Cybersecurity Skills

2.1 Cybersecurity Skills Shortage

A cybersecurity workforce study by ISACA's Cybersecurity Nexus (CSX) in 2017 showed in cases where companies normally receive between 60 to 250 applications for advertisements for non-cybersecurity positions, only 3 % of the surveyed organisations received more than 20 applications for each cybersecurity opening, while 59 % received an average of only five applications for each cybersecurity opening. This application rate is even worse if taken into account that 37 % of respondents stated fewer than one in four candidates have the qualifications to keep the company secure. It mostly takes six months or longer to fill the advertised position resulting in Europe having one third of their cybersecurity jobs unfilled. Most employers indicated they need candidates with technical skills and practical hands-on experience, resulting in the current emphasis on security certifications [2, 7]. The most difficult jobs to fill are those with additional requirements such as financial skills, and job requiring a security classification take more than 10 % to fill [8].

Trevor Halstead of Cybrary (online education and training provider), sums up the critical situation:"We really screwed things up this time. Somehow, we are in a situation where the sector of technology with the greatest potential negative impact on our lives, businesses, governments, peace, safety and security happens to have a severe deficiency of qualified people to fill its jobs," [4].

A lack of awareness of cybersecurity careers contributes to this critical shortage phenomenon; a study by Raytheon and the National Cybersecurity Alliance published in October 2015 indicated 67 % of men and 77 % of woman in the US and 62 % of men and 75 % of woman globally, did not receive any counselling in high school or secondary schools on careers in cybersecurity [4]. Jim Michaud from SANS highlights the fact that there is also an underrepresentation of woman in this field [4].

2.2 Cybersecurity Careers

Cybersecurity is a very broad field and can be classified in different categories according to the roles in the corporate environment. For each of these categories different skills, tools and techniques must be identified to advance career paths [6]. The Cybersecurity Skills Gap Analysis (CSGA) report, prepared by the Workforce Intelligence Network for South Michigan, defines four broad cybersecurity occupation categories, each associated with distinct aspects of cybersecurity; frontline cybersecurity, cyber-sensitive service, physical security and access, and indirect cyber-related workers [9].

The framework used by most companies in the US was established by the National Initiative for Cybersecurity Education (NICE), created by the National Institute for Standards and Technology (NIST). This framework provides a common, consistent lexicon that categorises and describes cybersecurity work in terms of seven categories: [9, 10]: Securely Provision, Operate and Maintain, Oversee and Govern, Protect and Defend, Analyse, Operate and Collect, and Investigate.

The CSGA report indicates the top cybersecurity occupations in demand in the US are cybersecurity analyst/specialists, cybersecurity engineer, auditors, network engineers/architects, and software developers [9, 10]. These occupations include the high-value skills that are in critically short supply, with the most scarce being intrusion detection, secure software development, and attack mitigation [1]. The largest number of postings (232,552) were part of the "Operate and maintain" category. The importance of the conceptualisation and the design of secure systems is reflected in the listings for "Securely Provision". The third most in demand skills are in the "Analyse" category. [9, 10].

The majority (89 %) of cybersecurity job positions require a bachelor's degree or higher [9]. The report of Intel Security, in partnership with McAfee, indicated that about half of the surveyed companies prefer at least a bachelor's degree in a relevant technical area to enter the cybersecurity field [1]. Computer science, engineering, management information systems, information technology, and business administration were the most prominent fields of study. The most common certifications required for frontline cybersecurity workers were Certified Information Systems Security Professional (CISSP), SANS/GIAC certification, and certified systems auditor. There is also a high demand for cybersecurity in the defence industry (more than 10 % of advertised position [11]) and therefore many postings required a security clearance [9].

2.3 Cybersecurity Professionals Requirements

Van Zadelhoff, [12] argues one of the main reasons for the critical shortage is that security businesses tend to recruit job candidates with traditional technology credentials, for example, college degrees. IBM's response to the shortage is to create "new collar jobs" where skills, knowledge and a willingness to learn is given priority over degrees. Cutting-edge technology, such as Artificial Intelligence (AI), is core in these jobs. AI not only provides a way to help overcome the skills shortage, but is also a step forward in the way employees will work and companies will defend themselves. AI is currently used to gather and correlate the insights from a huge number of sources which can be

used by security professionals to extract relevant information. Companies are already using IBM's Watson for Cyber Security to connect obscure data points humans cannot possibly identify on their own, enabling employees to find security threats 60 times faster than manual investigations [12].

The National Initiative for Cybersecurity Education for cybersecurity professionals identify cybersecurity workload and workforce requirements [13]. The best candidates and professionals possess a solid mix of business, communication and technical skills [3]. Loeb also suggests new pathways, other than degrees, to widen the talent pipeline. Soft and technical skills are equally important for the cybersecurity practitioner; the inadequacy of the normal science and engineering training has been expressed and there is presently an impetus to expand cybersecurity education. Cybersecurity education must be addressed and deployed more rapidly and more widely than Science, Engineering and Technology Education [14].

3 Cybersecurity Capability and Capacity Building

3.1 Government and Education

The International Telecommunications Union (ITU) conducted a survey, the Global Cybersecurity Index (GCI), providing insight into the cybersecurity engagement of sovereign nation states and showing the commitment of countries towards cybersecurity. Their methodology uses a cyber maturity metric to assess the various facets of nations' cyber capabilities [15, 16].

According to the GCI, the five most advanced countries are those listed in **Table 1**, and the top five African countries are listed in **Table 2**. Detailed information on Tunisia is not provided in the report, and Egypt and Tunisia were included in the Arab region.

Table 1. Global Security Index 2017. Top five most committed countries [16]

Country	GCI Score	Legal	Technical	Organi-zational	Capacity Building	Cooper-ation
Singapore	0.92	0.95	0.96	0.88	**0.97**	0.87
United States	0.91	1	0.96	0.92	1	0.73
Malaysia	0.89	0.87	0.96	0.77	1	0.87
Oman	0.87	0.98	0.82	0.85	0.95	0.75
Mauritius	0.82	0.85	0.96	0.74	0.91	0.70

Table 2. Global Cybersecurity Index 2017 Top five most committed African Countries [16]

Country	GCI Score	Legal	Technical	Organi-zational	Capacity Building	Cooper-ation
Mauritius	0.83	0.85	0.96	0.74	0.91	0.7
Egypt	0.77	0.92	0.92	0.4	0.92	0.7
Rwanda	0.6	0.6	0.71	0.79	0.66	0.28
Tunisia	0.59					
Kenya	0.57	0.75	0.73	0.36	0.41	0.6

To determine the Capacity Building measurements, countries were evaluated on standardisation bodies, cybersecurity good practices, R&D programs, public awareness campaigns. professional training courses, national education programs and academic curricula, incentive mechanisms and the home grown cybersecurity industry [16]. These results are given in **Table 3** and **Table 4** - the level of commitment ranges from the highest (green/dark grey) to the lowest (light red/grey).

Table 3. Top five countries in the World - Global Cybersecurity Index for Capacity building,

	Score	Global Rank	Standardisation bodies	Cyber-security good practices	R&D programmes	Public Awareness campaigns	Professional Training Courses	Educational pro-grammes	Incentive mecha-nisms	Home-Grown in-dustry	**CAPACITY BUILDING**
Singapore	0.078	145									
United States	0.432	67									
Malaysia	0.069	148									
Oman	0.430	68									
Mauritius	0.83	6									

Table 4. Top five countries in Africa - Global Cybersecurity Index for Capacity building

	Score	Global Rank	Standardisation bodies	Cyber-security good practices	R&D programmes	Public Awareness campaigns	Professional Training Courses	Educational pro-grammes	Incentive mecha-nisms	Home-Grown in-dustry	**CAPACITY BUILDING**
Mauritius	0.83	6									
Egypt	0.772	14									

	Score	Global Rank	Standardisation bodies	Cyber-security good practices	R&D programmes	Public Awareness campaigns	Professional Training Courses	Educational programmes	Incentive mechanisms	Home-Grown industry	**CAPACITY BUILDING**
Rwanda	0.602	36									
Tunisia	0.591	40									
Kenya	0.574	45									

The CGI shows governments across the globe initiated several programs to alleviate cybersecurity shortages. However, in a study by the research firm Vanson Bourne, all 775 respondents indicated cybersecurity education was deficient and 76 % indicated that their government was not investing enough in cybersecurity talent [1]. The key success factor is the availability of cybersecurity education for individuals in the pipeline and the workforce; therefore the adaptation of training programs to include cybersecurity content and the development of new cybersecurity qualifications are vital factors. The Australian minister of education announced that the government will invest $4.5 million in Cybersecurity education centres to enhance cybersecurity careers. Theses Academic Centres of Cybersecurity in Australia have the aim to to enhance cybersecurity research and produce work-ready graduates. Survey results in Australia has shown that two thirds of Australian young adults have never discussed a career in cybersecurity in the high school [17]. The Department of Energy in the US indicated that they will also provide $25 million for cybersecurity education .

Current research shows that most educational institutions do not prepare students for a career in cybersecurity [1, 17, 18]. Exposure to cybersecurity careers is crucial for the development of interest in the field. Education, including practical hands-on training in cybersecurity, must start at an early age (in school) and target a diverse range of students. These programs, which should also be available at universities, will create awareness of potential cybersecurity careers and can also identify promising recruits for cybersecurity professions. It is important to generate interest and enthusiasm among people with the skills, knowledge, and aptitude to fill cyber positions [14]. Currently curricula is not updated fast enough due to staffing difficulties, lack of budget and politics. Universities must be enabled to set up their students with tools to be successful Cybersecurity practitioners [18]. Universities must work with industry and government to tailor curricula that include practical training. These potential partnerships can leverage private sector talent in training teachers, enhancing curricula, and in offering internship and training opportunities to talented high school and university students, and can be mutually beneficial [1]. Cybersecurity curricula have to follow an integrated and multidisciplinary approach with emphasis not only on technology but also on the role of humans, processes, organisations and governance. Curricula for cross-cutting cybersecurity curricula must be developed that will introduce core principles, such as threat awareness and planning; cybercrime and computer forensics; security practices and principles; safety, privacy and ethics; and online interaction.

Although university degrees are necessary, additional pathways are required to widen the pipeline [1]. Businesses to start investing in both short courses and formal qualifications for the development of cybersecurity skills.

Research is an essential part of the cyber environment. Collaboration between industry, research institutions and universities can establish interdisciplinary faculty teams to conduct projects with the goal of developing university-industry relationships and create a platform to access larger-scale industry and government research funding. It can initiate dialogue between industry members and academic members about future cyber security threats and workforce requirements in order to develop new content for cyber security education.

Competitions are a critical part of cyber education. Companies expect proof of cybersecurity skills; in the case of cyber, skills are best built in lab environments where individuals can respond to real threat scenarios. “When you’re protecting the data for thousands, or perhaps millions, of individuals, “learning on the job” just won’t cut it anymore” [3]. The social and gaming aspects of cyber competitions are particularly compelling to the youth and is a valuable tool in cyber workforce development. During these games, both offensive and defensive skills are used in a sandboxed environment (real world) with no influence on the company or online systems. In addition, participants learn the soft skills of leadership, communication, critical/analytic thinking, teamwork, and creativity that are desirable characteristics in a cybersecurity role. Recruiters sometimes observe candidates during these games and candidates with these skills often get job during the competitions [14]. Jessica Gulick, CEO of Katzcy Consulting, emphasised this point by stating: “Cyber games train us to know what we’re looking for, as well as how best to respond. By developing cyber teams that compete in games like sports teams do, we can establish a code of ethics and a non-military approach focused on collaboration and strategy that will create the workforce we need for the future.” [6].

Imprecise job descriptions and the lack of metrics to assess skills complicate the recruitment process for cybersecurity jobs. There is often a mismatch between job descriptions and actual duties that creates unhappiness in the workforce [1]. Although the US has provided the NIST Cybersecurity Workforce Framework, most job descriptions in other countries are not yet standardised across the public and private sectors [1].

Government should consider collaboration with the private sector to enhance training opportunities for students. These programs include bursaries for potential students, private sector internships, and co-operative education programs for university students studying in science and technology [1]. Raising awareness and formal studies will increase the number of trained people, but it will take some time to have an effect. People in mid-career from other fields can be converted through assessment tools and offered training [14]. Training programs must be developed on a national level to address the need, and they should engage a diverse workforce, including women and veterans, and offer flexible working conditions [14]. The CSIS study has shown the lack of minorities in cybersecurity occupations. The workforce can also be expanded by increasing the number of working visas in this field [1].

3.2 Business

In a future world where cutting-edge technology is at its core, businesses need to change their approach in order to accommodate the new cyber-related jobs. Companies need to be strategic in deciding what skills will be needed to combat future cybersecurity threats and how new technologies can offset workforce shortages. To accomplish the shift from knowledge-based learning to skills-based training, organisations need to invest in their workforce. Although this type of training is expensive, the outcome of such investment will be experienced cybersecurity professionals [3]. Companies interested in adopting a "new collar" approach to fill security positions should consider the following:

- Re-examine their workforce strategy, identify the skills needed, and where those skills can be sourced from. This will also influence future recruitment processes [12].
- Start robust support programs for new employees that can include mentorships and the shadowing of experienced cybersecurity employees. Expose new employees to varied projects to broaden their cybersecurity knowledge. This support can include advice about expectations in the industry, cybersecurity roles, work shadowing skills requirements and other training opportunities [12].
- Groom employees with tangential skills—such as application specialists and network specialists—to move into cybersecurity positions. Creating such career paths can be a solid investment, as it can be cheaper to fill the gaps and enhance employee morale [2].
- Redefine minimum credentials for entry-level cybersecurity jobs by relaxing degree qualification requirements and accept non-traditional types of education (certifications) since universities do not currently offer sufficient cybersecurity programs [1]. Open additional pathways to cybersecurity careers to widen the talent. Despite the stigma attached to hacking, employers can consider employing previous hackers [1].
- Focus on continuous learning and upskilling the current workforce because cybersecurity is a highly dynamic field that requires ongoing education and exploration. Many new professionals lack the necessary skills and even proficient workers will require continuous skill development. Employers are increasingly providing on-the-job training [1].
- Retain employees by keeping them informed through classes, certifications, and conferences. Employees may reluctant to enroll employees for expensive training courses because they may be recruited by other companies. However, the absence of training is often a significant factor in a decision to seek alternative employment [1]. Studies show substantially more women leave the field early than men [3]. Create a culture of talent maximisation to retain staff. Even when budgets are tight, initiatives such as alternative work arrangements, investment in personnel growth and technical competency, and job rotation help to round out skills and minimise frustration with repetitive (but necessary) tasks. Invest in performance-based mechanisms for hiring and retention processes [2].
- Employers should grow skills in response to anticipated needs, including automation of some functions from "human in the loop" to "human on the loop" processes, to

reduce the current the burden on existing cybersecurity staff. Although automation cannot replace the human judgement, cybersecurity staff must adapt their skills to this increasing automated environments and focus their time and talent on the more advanced threats that require human intervention [1]. Automation of operational security tasks can decrease the overall burden on staff. AI provides employees with more intelligence and contextual recommendations at a speed and scale previously unimagined, so upskilling your workforce is now a completely different ballgame [12].

- Practical skills for cybersecurity can be enhanced through cybersecurity exercises. These exercises can be developed to simulate real-life cyber situations where participants will gain insight into the causes of the cyber-attacks and the effects and recovery after a cyber-attack.
- Business can support cybersecurity career development by building a local cybersecurity ecosystem and influencing early career thinking of young cybersecurity talent. Business must connect with government organisations, educational institutions, and other groups; they can contribute ideas to teachers about topics and activities to include in the curriculum, sponsor Capture the Flag security events, and work with schools to generate interest in the field. These groups are always looking for willing experts and mentors [12]. Engagement with and cultivation of students and career changers are encouraged and can done through university outreach or internship programs [2].

There are many benefits for business to become involved in cybersecurity career development, even from efforts focused on the development of national Capabilities and capacity:

- Employers that participate in cybersecurity collaborations will have increased visibility and enhance their profile and reputation amongst learners and parents. Their interactions with educational institutions will promote cybersecurity as a socially responsible profession. Investment in new talent will also contribute to the building of links between businesses and universities.
- During the development of young peoples' skills, knowledge and understanding of applications in the real world, business can tap into the creative thinking of young people.
- Employers can get early access to promising technology graduates with the required skills by engaging with potential recruits early in their degrees and potentially save on graduate recruitment costs.
- Engagement in outreach activities will provide career development opportunities for their cybersecurity employees e.g. communication, planning and presentation skills.
- By providing internships, cybersecurity employers can help shape the skill of future cybersecurity professionals, get a head start in recruiting the most motivated students, bring enthusiasm and a fresh approach to their business, and create a cost effective way to add additional resources to a team. After the internship period, employers can recruit interns for who are already up-to-speed with the business.

3.3 South Africa

South Africa is not an exception in this skills shortage phenomenon; there is only a small pool of experienced cybersecurity professionals and local businesses compete for those skills. If the country aims to be equipped to respond to cyber-threats and have a growing cybersecurity sector, it needs to strengthen the pipeline of cyber talent and help to prepare students for entry-level security career opportunities. This a specific opportunity for industry to work with the education sector and the government in order to adopt an innovative and exciting approach to teaching cybersecurity skills and creating learning materials on topics such as developing safe and secure software.

The Cybersecurity Centre of Innovation (CCOI), recently established by the Council of Scientific and Industrial Research (CSIR) follows an integrated and multidisciplinary approach to the challenge of cybersecurity capability and capacity building, with an emphasis not only on technology but also on the role of humans, processes, organisations and governance. Several workshops were held to support higher education institutions to develop new cybersecurity qualifications. However, the development of a cybersecurity capability for South Africa cannot be attained by a single party. Researchers, government, industry, the private sector and academia should join forces and create public-private partnerships to share their knowledge and support the development.

Schools

Government and business can influence the early career thinking of potential young cybersecurity talent and learning in schools. School children should be inspired to follow cybersecurity careers to contribute to a robust pipeline for universities, Technical and Vocational Education and Training (TVET) colleges and new entrants to the industry. Cyber professional can influence learners and challenge stereotypes about the cybersecurity career paths of skilled people. Curricula for cyber science that introduce the core principles such as threat awareness and planning, cybercrime and computer forensics, security practices and principles, safety, privacy and ethics, and online interaction, must be developed.

Business can support workshops or cyber camps for school learners where cybersecurity experts can teach students about cybersecurity threats and defences. These workshops should include cross curricular concepts e.g. the law and use resources such as board games, mobile apps and online games to maintain excitement. Cybersecurity exercises can be developed to simulate real life cyber situations where practical experience can be gained on the causes of the cyber-attacks, and the effects and recovery after a cyber-attack, and professionals can support the content with examples of real-life scenarios. The CSIR is already collaborating with universities on conducting cybersecurity games.

Cybersecurity professionals and employers can also support mentoring programs for teachers and the development of teaching resources. In addition, a cyber-aware accreditation pathway can be created for teachers and children. Information on the role of cybersecurity professionals in an organisations, the remuneration for these careers and both technical and non-technical career paths can be included.

Higher Education

Currently, Information Security in South Africa are mostly offered via short courses, or specialisation modules in Masters Degrees. New cybersecurity education opportunities must be created in the higher education sector to develop capacity and capability; cross-curricular concepts in cybersecurity modules and subjects in current qualifications, and the development of new focused cybersecurity qualifications. Programmed must be adapted to include new educational approaches including online courses and collaborative environments for cyber education. One of the reasons for the absence of formal qualifications at universities, is the lack of infrastructure and resources (teaching and research). Exchange programs for lecturers, researchers and students can enhance such capacity development and will support the development of these new degree and diploma programs in cybersecurity.

Business

There must be collaboration between industry, universities and government to build a sustainable knowledge-based workforce that support the needs of government, industry, and academia. The active engagement of businesses in research as part of the CCOI, will build a trusted relationship between them and higher education researchers that can solve their needs and, over time, enable ideas and techniques from the academic domain to be applied to industrially relevant problems in cybersecurity with the benefit of prompt exploitation of high quality cybersecurity research. Businesses can fund research projects in the CCOI, donate facilities to universities to accelerate innovation and support two-way secondments between university and academia.

The Network Emulation and Simulation Laboratory (NESL) is a simulation and emulation environment that is used for online emulation and simulation of networks and the testing of cybersecurity software and equipment developed by the CSIR. This platform can be used by companies to run cyber exercises for their cybersecurity employees. It is important that cybersecurity professionals from industry support these initiatives with examples of real-life scenarios that will ensure relevance and attractiveness of educational resources.

It is widely recognised that there is a need for a closer working relationship between academia and businesses in order to make educators aware of the developments in cybersecurity. Such collaboration will ensure that both undergraduate and postgraduate degrees meet business needs and help universities to develop programs that are directly linked to the knowledge and skills that cybersecurity jobs require. The courses should provide a strong foundation of cybersecurity knowledge but must also build hands-on skills [3]. Courses at TVET colleges can include first level technician programs for constant monitoring of a company's devices and systems to detect and deal with any security weaknesses.

Industry should support higher education institutions with curriculum development and other training processes (e.g. workshops), employers can get early access to promising technology graduates with the skills they want by engaging with potential recruits early in their degrees and potentially save on graduate recruitment costs. In addition, industry can support the development students' skills, knowledge and understanding of

applications in the real world. Cybersecurity professionals can contribute ideas to lecturers about topics and activities to include in the curriculum.

Provision must also be made for bursaries, studentships and internships. The internships should be between 6 and 12 months in duration, and suitable either for undergraduates taking IT-related degrees, or for recent graduates. To make the most of internships, employers must have meaningful work for an intern to do, be willing to provide support such as a line manager.

4 Conclusion

This paper considers various actions required to build capability and capacity for cybersecurity in South Africa in addition to a discussion of the obstacles that have to be overcome to achieve this goal. The critical cybersecurity skills shortage is a global problem and South Africa is no exception. This paper considers measures for governments, business and academia to alleviate the shortage, and pay particular attention to the South African case.

To ensure a larger and more diverse cybersecurity workforce, countries need to develop critical technical skills, cultivate a more diverse workforce, and reform education and training programs. The results of the Global Cybersecurity Index imply that South Africa needs to enhance their commitment to cybersecurity capability development. There is a role for government, business and academia in the development of the required capabilities. Universities and colleges must be supported to initiate new cybersecurity qualifications. It is also important to enhance the role of businesses in capability building initiatives such as the participation in cybersecurity awareness in schools as well as be involvement in the career choices of young people. Businesses can support the development of curricula to also include information on the latest threats and attacks. The implementation of cybersecurity exercises gives opportunities of hand-on learning and can enhance interest in these careers. In addition, business can sponsor bursaries and support internships.

Cybersecurity is a complex career field with extraordinarily challenging problems, but with a diverse pool of experiences and ideas, we stand a much greater chance of successfully defending our assets.

References

1. Intel Security, in partnership with the Center for Strategic and International Studies, https://www.csis.org/programs/technology-policy-program/cybersecurity-and-warfare/other-projects-cybersecurity-0
2. HelpNetSecurity, https://www.helpnetsecurity.com/2017/02/13/cyber-security-skills-gap-tips/
3. Media Planet future of Business and Tech, http://www.futureofbusinessandtech.com/online-and-mobile-safety/5-steps-to-closing-the-cybersecurity-skills-gap
4. CIO, https://www.cio.com/article/3005637/cyber-attacks-espionage/closing-the-cybersecurity-talent-gap-one-woman-at-a-time.html

5. TREND MICRO, https://blog.trendmicro.com/the-challenges-of-cyber-security-education-and-training-in-2015/
6. Ricci, M., Gulick, J.: Cybersecurity Games: Building Tomorrow's Workforce. Journal of Law & Cyber Warfare 5, 183 (2017)
7. ISACA, http://www.isaca.org/cyber/Documents/CSX-General-Awareness-Brochure_Bro_Eng_0816.pdf
8. http://fortifyexperts.com/employment-trends/cybersecurity-employment-trends/
9. https://winintelligence.org/wp-content/uploads/2017/07/FINAL-Cybersecurity-Skills-Gap-2017-Web-1.pdf
10.National Initiative for Cybersecurity Careers and Studies, Department of Homeland Security, https://niccs.us-cert.gov/nice-cybersecurity-workforce-framework-work-roles
11.Burning Glass Technologies, burning-glass.com/wp-content/uploads/Cybersecurity_Jobs_Report_2015.pdf
12.Harvard Business Review, https://hbr.org/2017/05/cybersecurity-has-a-serious-talent-shortage-heres-how-to-fix-it
13.NICE: Best Practices for Planning a Cybersecurity Workforce White Paper. In: Security, H. (ed.), (2014)
14.Katchy Consulting: CYBERSECURITY GAMES: BUILDING TOMORROW'S WORKFORCE. In: NIST (ed.), (2016)
15.International Telecommunications Union (ITU), https://www.itu.int/en/ITU-D/Cybersecurity/Documents/2017_Index_of_Indices.pdf
16.International Telecommunication Union, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf
17.ZDNeT, https://www.zdnet.com/article/australia-to-spend-au4-5m-on-cybersecurity-education-centres/
18.CIO, https://www.cio.com/article/3060813/it-skills-training/top-u-s-universities-failing-at-cybersecurity-education.html